WINTER 2023

PALO ALTO NETWORKS

CYBER PERSPECTIVES

2023 CYBERSECURITY PREDICTIONS FOR WHAT'S TO COME

LATEST RESEARCH
What's Next in Cyber: A Global Executive Pulse Check

ECONOMICS
Making Cybersecurity the Smart Investment in an Era of Economic Uncertainty

5G
What Can Service Providers Do About 5G Security?

SYMPHONY
2023

Journey to the Modern SOC

The premier summit for security operations.

February 22–23, 2023

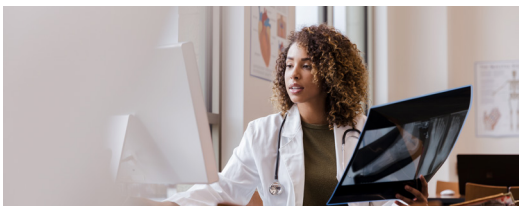
Register Here

presented by:

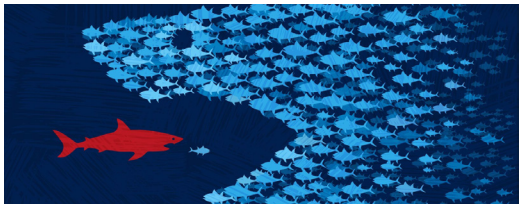
paloalto® NETWORKS | CORTEX® BY PALO ALTO NETWORKS

LATEST RESEARCH

CYBER LEADERSHIP



ZERO TRUST



CYBER STRATEGY

ECONOMICS

5G

paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization

By Aveek Das

Executive Summary

Unit 42 recently set out to better understand how well hospitals and other healthcare providers are doing in securing smart infusion pumps, which are network-connected devices that deliver medications and fluids to patients. This topic is of critical concern because security lapses in these devices have the potential to put lives at risk or expose sensitive patient data.

We reviewed crowdsourced data from scans of more than 200,000 infusion pumps on the networks of hospitals and other healthcare organizations using IoT Security for Healthcare from Palo Alto Networks.[1] An alarming 75 percent of infusion pumps scanned had known security gaps that put them at heightened risk of being compromised by attackers. These shortcomings included exposure to one or more of some 40 known cybersecurity vulnerabilities and/or alerts that they had one or more of some 70 other types of known security shortcomings for IoT devices.

One of the most striking findings was that 52 percent of all infusion pumps scanned were susceptible to two known vulnerabilities that were disclosed in 2019 – one with a "critical" severity score and the other with a "high" severity score.

There is already a vast array of information about known vulnerabilities and approaches for securing these devices, thanks to the efforts of medical equipment makers, security researchers, cybersecurity vendors and regulators who have spent the past decade working to better understand cyber risks associated with use of infusion pumps and other connected medical devices. For example, the U.S. Food and Drug Administration (FDA) announced seven recalls for infusion pumps or their components in 2021,[2] and nine other recalls in 2020.[3]

There are also initiatives led by industry[4] and government[5] aimed at standardizing device information[6] and establishing baseline security criteria for manufacturing these devices. Yet the average infusion pump has a life of eight to 10 years, which means the widespread use of legacy equipment has hampered efforts to improve security. Other factors also continue to undermine overall security hygiene – including insufficient use of network segmentation, failure to implement »

best practices for securing operational processes and insufficient security training for healthcare workers.

Our discovery of security gaps in three out of four infusion pumps that we reviewed highlights the need for the healthcare industry to redouble efforts to protect against known vulnerabilities, while diligently following best practices for infusion pumps and hospital networks.

Healthcare providers are protected against the vulnerabilities discussed here by the Palo Alto Networks IoT Security platform through the identification of managed and unmanaged devices and risks associated with those devices, the application of risk reduction policies and built-in prevention of known threats, as well as detection of and response to unknown threats.

CVEs discussed	CVE-2019-12255, CVE-2019-12264, CVE-2016-9355, CVE-2016-8375, CVE-2020-25165, CVE-2020-12040, CVE-2020-12047, CVE-2020-12045, CVE-2020-12043, CVE-2020-12041
Related Unit 42 topics	IoT devices

Severity of Infusion Pump Vulnerabilities

Infusion pumps can number in the thousands in a large hospital or clinic, and recalls, whether due to mechanical failure or cybersecurity vulnerability, can be a source of anxiety for supply chain managers, clinical engineers and IT security teams. The at-risk devices must be identified, found and retired or repaired per the instruction of a given recall. An oversight or a miss in any of these areas – whether the devices need repair, maintenance, software patches or updates – can put patient lives or sensitive information at risk.

We recently analyzed more than 200,000 infusion pumps from seven medical device manufacturers using crowdsourced data supplied by customers using Palo Alto Networks IoT Security for Healthcare[7] to see how many and what types of security vulnerabilities these devices have. In this analysis, the Palo Alto Networks IoT Security platform identified over 40 different vulnerabilities and over 70 different security alerts among the devices, with one or more affecting 75% of the infusion pump devices we analyzed. Here we focus on the threats and vulnerabilities we observed most commonly among that group.

The table below identifies the 10 most prevalent vulnerabilities from analysis of the scan data. It lists the CVE number, severity score and percentage of pumps scanned that were susceptible to that vulnerability. 52 percent of the devices we scanned were flagged as being vulnerable to the top two CVEs, which were publicly disclosed in 2019 and have severity scores of "critical" and "high." »

Table 1: Top 10 Infusion Pump Vulnerabilities and Percentage of Vulnerable Infusion Pumps as Identified by Palo Alto Networks IoT Security

	CVE	Severity (Score)	% of analyzed pumps with CVEs
1	CVE-2019-12255[8]	9.8 (Critical)	52.11%
2	CVE-2019-12264[9]	7.1 (High)	52.11%
3	CVE-2016-9355[10]	5.3 (Medium)	50.39%
4	CVE-2016-8375[11]	4.9 (Medium)	50.39%
5	CVE-2020-25165[12]	7.5 (High)	39.54%
6	CVE-2020-12040[13]	9.8 (Critical)	52.11%
7	CVE-2020-12047[14]	9.8 (Critical)	52.11%
8	CVE-2020-12045[15]	9.8 (Critical)	52.11%
9	CVE-2020-12043[16]	9.8 (Critical)	52.11%
10	CVE-2020-12041[17]	9.8 (Critical)	52.11%

Note: Five of the CVEs listed in Table 1 are previously disclosed vulnerabilities that could impact BD Alaris infusion pumps. These vulnerabilities were originally disclosed by the manufacturer in 2017, 2019 and 2020, and corresponding bulletins are available on the BD Cybersecurity Trust Center.[18] Links to each bulletin can also be found in Appendix A at unit42.paloaltonetworks.com/infusion-pump-vulnerabilities. BD has made software updates available to remediate these vulnerabilities and encourages customers to update to BD Alaris PCU version 12.1.2, which became available in July 2021. The remaining five vulnerabilities listed in Table 1 are unrelated to BD products.

Types of Vulnerabilities Observed in Infusion Pumps

The most common vulnerabilities we observed that are specific to the infusion systems we studied can be grouped into several categories according to the effects they may have: leakage of sensitive information, unauthorized access and overflow. Other vulnerabilities stem from third-party TCP/IP stacks but can affect the devices and their operating systems.

Leakage of Sensitive Information

We observe that a large number of vulnerabilities in infusion pump systems – and in Internet of Medical Things (IoMT) devices overall – are related to leakage of sensitive information. Devices vulnerable to this type of issue can leak operational information, patient-specific data, or device or network configuration credentials. Attackers looking to exploit these vulnerabilities need varying degrees of access. For example, CVE-2020-12040, which is specific to clear-text communication channels, can be remotely exploited by an attacker via a man-in-the-middle attack to access all the communication information between an infusion pump and a server. On the other hand, CVE-2016-9355 and CVE-2016-8375 can be exploited by someone with physical access to an infusion pump device to gain access to sensitive information – which makes the attack less likely, but still possible for an attacker with specific motivations.

Overflow and Unauthorized Access

Other vulnerabilities related to overflow or incorrect access control can give unauthenticated users an ability to gain access to a device or to send network traffic in a certain pattern that can cause a device to become unresponsive or operate in a way that is not expected – and in healthcare organizations, this can potentially mean causing a disruption to hospital operations and patient care. Also, the possibility of unauthorized access isn't limited to the successful exploitation of vulnerabilities. Continuous use of default credentials, which are readily available online via a simple search, is another major issue in IoT devices in general – since it can give anyone who is in the same hospital network as the medical devices direct access to them.

Vulnerabilities in Third-Party TCP/IP Stacks

Finally, it is not only sufficient to be aware of vulnerabilities in the infusion systems themselves. Many IoMT (and IoT) devices and their operating systems use third-party cross-platform libraries, such as network stacks, which might have vulnerabilities affecting the device in question. For example, for CVE-2019-12255 and CVE 2019-12264, the vulnerabile TCP/IP stack IPNet is a component of the ENEA OS of Alaris Infusion Pumps, thereby making the devices vulnerable.

Common Security Alerts in Infusion Systems

Overall, most of the common security alerts raised on infusion systems indicate avenues of attacks that the device owner should be aware of, for example, via internet connections or via default username and password usage. On the other hand, with ML-driven continuous monitoring, any anomalous behaviors on infusion systems can quickly identify potential attacks in progress. Flagging devices displaying anomalous behavior or misuse is crucial to identifying zero days or live attacks on the system.

Below are the security alerts we observed most commonly in the infusion pumps we analyzed. »

Table 2: 10 Most Commonly Observed Security Alerts in Infusion Systems by Palo Alto Networks IoT Security

	Alert Title	Impact and Relevance
1	Excessive count of TCP reset packets sent from unestablished connections	A large number of reset packets sent from connections outside the local network can indicate a continuous attempt at a connection to an unauthorized destination, which could indicate anomalous behavior on the device.
2	Invalid User-Agent string (garbage values) observed in an HTTP request in IoMT device	Garbage values in the User-Agent string can indicate suspicious behavior. This means that the network connection between the infusion system and the corresponding destination should be monitored more closely.
3	Unencrypted sensitive login information observed in an HTTP request	Sensitive information via HTTP (which is a non-encrypted protocol) can be easily monitored by a malicious actor and can leak information related to device/patients.
4	Manufacturer factory default username and password in inbound HTTP login	Use of factory default credentials to log in to a device via HTTP is a serious security concern. These credentials can be easily found online or in manuals and anyone can access them.
5	Suspicious (high and not commonly observed) port number in network traffic	Anomalous port numbers and counts observed in incoming and outgoing traffic in the infusion system. Such anomalous behavior indicates that the device should be more closely monitored.

Table 2: 10 Most Commonly Observed Security Alerts in Infusion Systems by Palo Alto Networks IoT Security (continued)

	Alert Title	Impact and Relevance
6	Unsecured outbound HTTP connections from IoMT device to the internet	Outbound connections to the internet (outside the local network) via HTTP (which is non-encrypted) should be avoided for all infusion systems. Communication should be limited to devices inside the hospital network/specific medical VLAN.
7	FTP anonymous login (without specific username/password) via local network	Anonymous login without proper credentials can indicate malicious behavior, and the device should be flagged.
8	Manufacturer factory default username and password in the inbound FTP login	As observed for HTTP, factory default credentials for FTP are a similar security no-no.
9	Unsecure outbound FTP connections from IoMT device to the internet	Similar to outbound HTTP connections from medical devices to the internet, FTP connections outside the hospital network could make the device susceptible to attacks.
10	Unsecure HTTP service hosted on the IoMT device	Hosting an HTTP service on an infusion system, which is a mission-critical medical device, as well as holding sensitive data, makes the device prone to security attacks.

Proactively Secure Your Infusion Pumps

For healthcare providers, keeping vulnerable IoMT devices safe from known and unknown threats goes beyond device identification and alerting. The sheer volume of devices in the healthcare environment makes an alert-only approach risky and impractical. In addition, alert-only solutions require integration with third-party systems for prevention adding to the complexity of deploying and managing these systems over time. Healthcare security teams require IoT security technology with built-in prevention that secures even unmanaged devices.

The pervasiveness of the threats, the volume of devices in service, and the lack of visibility into device risks and behavior combine to make the security challenges seem insurmountable. Here's the good news: With the right strategy and the right security technology, healthcare IT and clinical engineering teams can get the visibility they need to manage and secure all IoMT devices and ensure patient safety.

Here are some key capabilities to consider when evaluating IoMT security strategies and technologies for healthcare.

1. **Accurate discovery and inventory**: Teams must be enabled to quickly discover, locate and assess utilization of all infusion pumps, including mobile and rental equipment. The discovery of infusion pumps supports accurate inventory that can also be shared with asset management or computerized maintenance management system (CMMS) solutions like ServiceNow. Utilization insights can help with procurement planning and eliminating costly underutilized rental equipment. A location feature comes in handy when planning preventive maintenance or manually applying remediation of an issue.
2. **Holistic risk assessment**: Holistic risk assessment helps security teams proactively find vulnerabilities and identify compliance gaps. A system capable of delivering machine learning-driven insights can help establish a behavior baseline and provide a deep risk assessment. This could include watching for threat indicators (e.g., an abnormal connection between devices or the presence of malicious files. It could also mean monitoring for issues such as default passwords, end-of-life operating systems, apps or devices, and obsolete protocols. It's also important to monitor CVEs and assess them in context, taking account of additional factors such as FDA recalls, MDS2 information, ePHI information, vendor patching information, patch level and so on. Finally, a risk assessment strategy can be strengthened by extended capabilities achieved through integrations with third-party vulnerability management systems such as Qualys, Rapid 7 and Tenable to scan for additional vulnerabilities in infusion pumps.
3. **Apply risk reduction policies**: Real-time risk monitoring, reporting and alerting are crucial for organizations to proactively reduce IoMT risk. Consistent profiling of device activity and behavior yields data that can be accurately converted into risk-based Zero Trust policy recommendations.[19] This approach enables security teams to confidently allow only trusted behavior, and if necessary, segment infusion pumps from other IT and medical devices to reduce attack radius. For example, as mission-critical devices supporting the lives of patients, such devices should have their own »

isolated VLANs for communicating with a server and clinical workstations – outbound traffic from such devices can be a real cause for concern, as it could indicate exfiltration of sensitive information.

4. **Prevent threats**: The diverse nature of IoMT devices will require actionable insights into detection and prevention of known threats against infusion pump devices for a swift response for threat mitigation. Built-in prevention capabilities help block known targeted IoT malware, spyware and exploits, preventing the use of DNS for C2, and stopping access to bad URLs or malicious websites to help prevent the loss of sensitive data.

Palo Alto Networks has been working with healthcare customers closely to help narrow security and compliance gaps across the health system.

Conclusion

Among the 200,000 infusion pumps we studied, 75% were vulnerable to at least one vulnerability or threw up at least one security alert. While some of these vulnerabilities and alerts may be impractical for attackers to take advantage of unless physically present in an organization, all represent a potential risk to the general security of healthcare organizations and the safety of patients – particularly in situations in which threat actors may be motivated to put extra resources into attacking a target.

With attack surfaces widening and attack vectors becoming more refined than ever before, now's the time for healthcare organizations to define medical device security with a new level of sophistication.[20] To successfully implement secure clinical and device workflow management that is scalable, yet practical to maintain and enforce, the methodology should also alleviate the escalating operational burdens of securing and managing medical devices for both network security and clinical support teams.

The IoT Security platform protects customers from these security risks by accurately identifying devices on the network; assessing risk by evaluating device profiles for vulnerabilities, exposures or security advisories; detecting anomalies with ML-driven continuous monitoring; and enabling built-in prevention for attacks exploiting these vulnerabilities, including known and unknown threats, with automated Zero Trust policy recommendations and enforcement.

1. https://www.paloaltonetworks.com/network-security/iot-security-for-healthcare
2. https://www.fda.gov/medical-devices/medical-device-recalls/2021-medical-device-recalls
3. https://www.fda.gov/medical-devices/medical-device-recalls/2020-medical-device-recalls
4. https://cmdc.umn.edu/
5. "FDA In Brief: FDA Issues Draft Guidance on Remanufacturing and Discussion Paper Seeking Feedback on Cybersecurity Servicing of Medical Devices," U.S. Food & Drug Administration, June 17, 2021.
6. Kalyan Siddam, "MDS2: A Treasure Trove for Internet of Medical Things (IoMT) Security," Palo Alto Networks, January 26, 2022.
7. https://www.paloaltonetworks.com/network-security/iot-security-for-healthcare
8. https://nvd.nist.gov/vuln/detail/CVE-2019-12255
9. https://nvd.nist.gov/vuln/detail/CVE-2019-12264
10. https://nvd.nist.gov/vuln/detail/CVE-2016-9355
11. https://nvd.nist.gov/vuln/detail/CVE-2016-8375
12. https://nvd.nist.gov/vuln/detail/CVE-2020-25165
13. https://nvd.nist.gov/vuln/detail/CVE-2020-12040
14. https://nvd.nist.gov/vuln/detail/CVE-2020-12047
15. https://nvd.nist.gov/vuln/detail/CVE-2020-12045
16. https://nvd.nist.gov/vuln/detail/CVE-2020-12043
17. https://nvd.nist.gov/vuln/detail/CVE-2020-12041
18. https://cybersecurity.bd.com/trust-center
19. *Zero Trust for Healthcare Organizations Overview*, Palo Alto Networks, May 27, 2022.
20. Danielle Kriz, "Governments Must Promote Network-Level IoT Security at Scale," Palo Alto Networks, December 8, 2021.

Aveek Das is a senior staff researcher working on IoT Security and Threat Prevention at Palo Alto Networks

What's Next in Cyber

A Global Executive Pulse Check

Even before the pandemic, remote work was growing in popularity; digital transformation was driving companies to the cloud; the proliferation of IoT devices was exposing new security vulnerabilities; and increasingly sophisticated cybercriminals were regularly exploiting new attack vectors.

The pandemic just shifted the need to address these challenges into overdrive. In the blink of an eye, hybrid work became the status quo. Unsecured third-party devices were being used everywhere. And a massive shift to multicloud environments left cybersecurity teams scrambling to secure more than ever against more cyberthreats than ever. To boot, talent shortages made doing so all the more difficult. At Palo Alto Networks, our vision is to make each day safer than the one before. As a means of making sure we continue to do so, it's important for us to know the concerns, priorities, and observations of the world's executives with regard to securing their organizations. To find out, we asked 1,300 C-suite leaders (CISOs, CIOs, CSOs, CTOs, and COOs) from around the globe and across different industries to share their thoughts and their wisdom. Their answers can be found in the 2022 Global What's Next in Cyber survey. In the pages ahead, we've pulled out some of the key data from the survey to help inform your own cyber transformation.

Here are some of our observations based on the results. On the one hand, organizations are racing toward modernizing their infrastructure, with software smart and fast enough to respond to current and future threats, and to achieve cyber resilience. On the other hand, not everybody is where they need to be. We understand that it can be difficult to know where to start or what to prioritize, but there are some critical areas where organizations need to move the dial. Leaders will need to make tough decisions and bold moves. Cyber transformation is only possible when CIOs and CISOs free themselves from the legacy security architectures of today and reimagine them for the future — one where the most complex and evasive threats are stopped in real time, at any scale. In the secure future, hybrid work is protected by secure access service edge (SASE), with continuous security delivered at scale. Artificial intelligence and machine learning automate anomaly detection, improve visibility and control, and counter zero-day attacks. And defending our digital way of life is simplified by integrated security platforms designed to protect the most critical areas of modern organizations.

At Palo Alto Networks, our goal is to help organizations leverage security as a strategic enabler of the business outcomes they desire. We want to be your partner in securing the way forward. We hope these survey results will shine a light on the path ahead so you can walk it with confidence and optimism.

The Growing Threat

These days, every organization is in the crosshairs of cybercriminals. Every new device, user, or piece of sensitive data expands the attack surface, giving threat actors more opportunities to compromise environments. And they're doing so with astonishing speed. Ransomware and business email compromise (BEC) are among the top attacks organizations will continue to face, with phishing and software vulnerabilities likely to remain the top means of access.

In the last 12 months

96%

of all respondents experienced at least one breach

57%

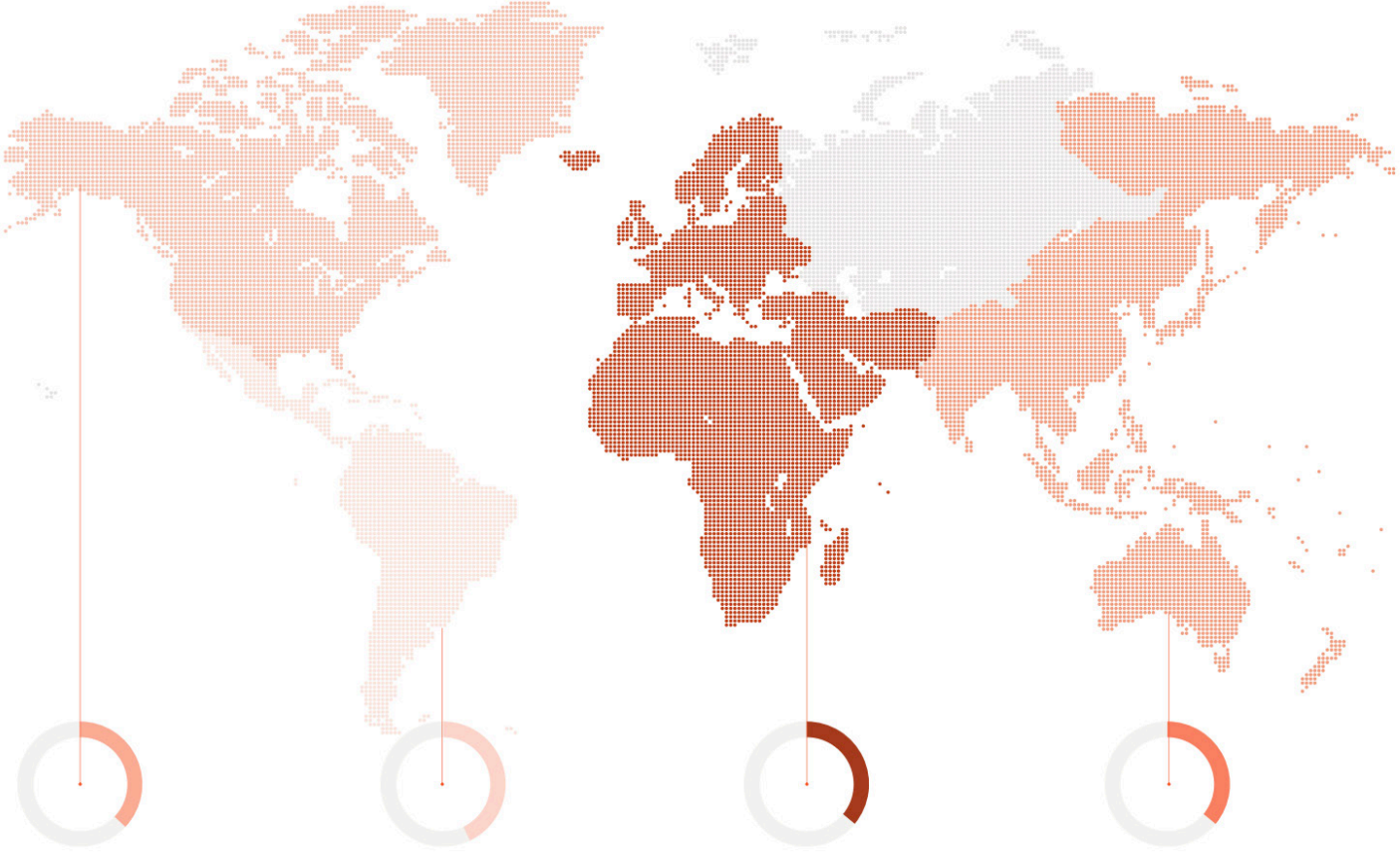
experienced three or more breaches

33%

of CISOs said they experienced an operational disruption as a result of a breach

84%

agree (to varying levels) that they have seen more security incidents due to hybrid work



The top reason CXOs cite for successful breaches, by region

NAM
Increase in hybrid/ remote work

LATAM
Insufficient threat detection and response capabilities

EMEA
Improving capabilities of cybersecurity adversaries

JAPAC
Insufficient threat detection and response capabilities

What Keeps Executives Up at Night?

According to the survey, only 25% of executives believe their organizations' cybersecurity readiness and resilience is high. We asked them to select their top three cybersecurity business priorities and the top three challenges for managing security across their organizations. It isn't surprising to see executives prioritizing automation and improved security operations, as 96% of those surveyed report a lack of skilled cyber professionals as one of their biggest challenges.

Executive Alignment Is Still an Issue

Eighty-nine percent of respondents say cybersecurity is on their boards' agenda at least once a quarter. However, lack of executive and board alignment and inadequate security governance across the organization must be addressed in order to truly manage cyber risk.

Vendors and Tools: Consolidation Is Coming

As organizations face a constant onslaught of cyberattacks, the complexity of managing vendors and point solutions creates security gaps. That explains why globally 77% of respondents said they are highly likely to reduce the number of security solutions and services they rely on. Going forward, we anticipate that cybersecurity teams will consolidate their vendor environments and pursue platforms that are comprehensive and scalable.

Investing in What's Next: Budgets and Resources

Globally, cybersecurity will continue to be a high-priority investment. As enterprises continue to rethink connectivity, we see them investing to protect 5G networks and the Internet of Things while turning to automation to improve productivity and operational efficiency.

Read the full report at www.paloaltonetworks.com/nextsurvey

paloalto NETWORKS | WE'VE GOT NEXT

How to Answer Your Board's Questions on Cyber Risk Mitigation

By David Faraone

When there is a cybersecurity incident, your board of directors wants to know if there is a plan. They want assurances that your organization is prepared to deal with the incident swiftly, efficiently, and thoroughly to minimize its impact on the business. That's why, after communicating about your cyber risk exposure, the next burning question you will likely need to answer will be around your cyber risk mitigation plan. You will need to be prepared to respond to the question, "Has the situation been contained and have we dealt with it adequately?"[1]

Subtext questions to consider:

- What was our response plan?
- How did we prioritize efforts and resource allocation?
- What is left to do?
- Were there any surprises and/or lessons learned?

Cyber Risk Mitigation: Are We Done?

What your executives and board really want to know is if the situation has been contained and what assurances you can provide that the risk has been dealt with appropriately.

To have a defensible position to answer questions like these from the board (or the audit committee in the future), you'll need documentation, documentation, and more documentation! Your incident response, patch management, and zero-day vulnerability plans will likely all be required to capture all the processes, communications, and steps taken to address and validate that the risk has been mitigated.

This documentation should be comprehensive, including not only the plans but also:

- The emergency change processes that you executed
- The people who were involved
- Patching and segmentation details (how and when systems were prioritized and patched/segmented)
- How systems related to critical processes
- How processes were stratified
- How enforcement rules were altered and deployed

The goal is to show exactly what was done, when, and how, so you can demonstrate due care and report the elements that your board, as well as regulators and auditors, are looking to understand.

Keeping Executives Informed: Recovery Is a Journey, Not a Moment

If the board asks, "Are you done? Is it contained? Did you finish up?" it's important to frame recovery as a journey, not a point-in-time experience. Recovery is an ongoing process that's about coming back stronger and faster.

This means you need to sit down and have the recap meetings that help you uncover lessons learned and figure out where you could have saved time or »

done something differently or better. When time is of the essence, the documentation that we've discussed is critical to making sure that nothing is missed, no stone left unturned, and no step left out. But it's also important to identify and then take care of the small stuff that can make a big difference in the efficiency of your operations.

For example, having easy-to-follow call trees for certain circumstances and business impact reports that tell you where your key assets are can save you a lot of time and effort when you're having the most stressful day of your life. Hindsight's 20/20, so take the time to figure out what would have been useful and then explain to the board what you are doing to come back stronger.

By framing your answers to the board's questions as a journey, you can remind them that security is never finished and never perfect, but it can keep getting stronger and more effective. Remember, "**the day of the dance is not the day to learn to dance**," so, in addition to documenting everything meticulously, don't forget to rehearse, rehearse, rehearse/practice, practice, practice, rinse and repeat. Let the board know how you are using every single opportunity to prepare and bolster your capabilities and what you are doing to make sure the next time will be even better (because, as we all know, there will always be a next time).

Check out part three of the series, which looks at how to answer, "What due diligence and assurances have we conducted?"[2]

1. https://www.paloaltonetworks.com/engage/communicate-cybersecurity-risks-with-your-board/situation-contained-adequately
2. LeeAnne Pelzer, "CISOs: How to Answer Your Board's Top Cybersecurity Questions—Cyber Due Diligence," Palo Alto Networks, accessed January 6, 2023.

David Faraone is a senior consulting director of Unit 42 at Palo Alto Networks

How to Answer Your Board's Questions on Regulatory Compliance Requirements

By LeeAnne Pelzer

So far, we've discussed how to talk to your board about cyber risk exposure, cyber risk mitigation plans, and due diligence in the event of an incident. The next logical set of questions you need to be prepared to answer is about cybersecurity regulatory compliance.

As we all know, our businesses are guided by a host of industry and government regulations. The moment you have an incident (or suspect a threat), it triggers an abundance of questions from many different entities around the potential impact on the security and integrity of your data and operations. You need to be prepared to effectively respond to these questions. Let's look at how to help prepare yourself to answer " **How are we going to reply to regulatory or other compliance inquiries**?"[1]

Subtext questions to consider:

- Do any potentially exposed systems process, store, or transmit regulated data?
- If so, who do we need to notify? Have we done so?
- What constitutes due care?
- How should remediation activities be tracked?

Cybersecurity Regulatory Compliance: What Do We Say and When?

From the moment a vulnerability is discovered, regulators will want to know how you assessed and mitigated your attack surface exposure. They will want to know details of your asset inventory, including if you can pinpoint where the vulnerability exists in your environment; what communications occurred; if there was a potential instance of compromise, and if so, was the appropriate regulatory authority »

notified in a timely manner; what mitigations and remediations were taken, any lessons learned, etc.

In a nutshell, regulators want to understand what existing processes you had in place and what actions you took to minimize the impact on any vulnerable assets. Often, when regulators are involved, it means customers and/or clients are also involved (e.g., their personally identifiable information has been stolen), or there is a potential systemic risk to your industry/sector (e.g., targeted attack on the energy grid). As a result, their inquiries are not something to be afraid of or shy away from—they just need to be responded to thoughtfully and transparently.

This will help minimize any potential for further damage (e.g., to your brand or reputation). If you had an exploit that impacted your organization (and your customers) and if you show how you dealt with it—tackled, addressed, and learned from it—it will paint the organization in a better light than if you try to hide it.

Communicating About a Cyber Incident: Know Who to Notify

Some regulations have provisions that dictate when regulated entities need to notify customers and specified third parties in the event of a breach. Sometimes contracts with third parties include notification provisions—they must notify you, or you have to notify them of an instance of exposure. However, you should also notify your crisis triage team, incident response vendor, and external counsel so they can take action.

Having an **incident response retainer**[2] is becoming almost standard practice, as it can help you demonstrate that you took reasonable steps to protect regulated data from exposure post-incident. In the event there is suspicion of exploitation or compromise, you will want to have the right retainer in place with a forensics and incident response firm, in addition to notifying your external counsel.

It is critical to make sure that all your communication protocols are bulletproof for all of your internal and external constituents. Note, a regulator will not expect you to have instantly remediated or mitigated incidents. What they are looking for is that you have done your due diligence upfront, so you weren't completely under-prepared. They want to know you were able to detect the attack and its impacts in a timely manner and worked with all the right stakeholders to communicate and remediate it.

Succeeding at Incident Response: It's All About Having Solid Relationships

When you are in the middle of dealing with an incident, you will find comfort in your existing relationships with external counsel and your incident response vendor. Reach out now and start building those relationships. Understand their triage processes and get their cell phone numbers. Do this proactively because when you are dealing with an incident, having one of your worst workdays, those strong relationships are going to be your lifeline.

Consider sharing your incident response plan[3] with your incident response vendor and get their thoughts. Bring them into the fold, so when these specialists come in and carry out that full investigation, you understand what they are doing and have some assurances that they can determine what has happened.

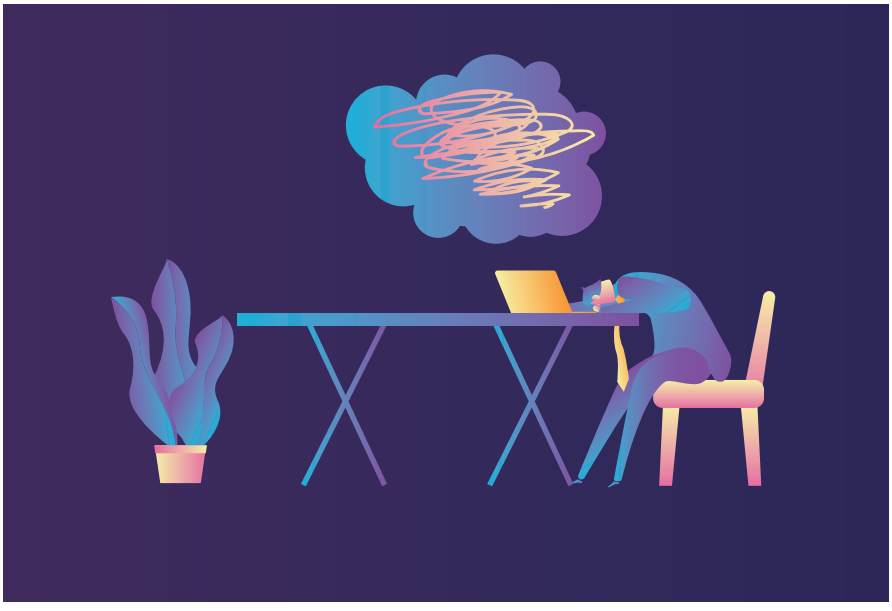
You want to be familiar with your retainer—make sure it includes activities that could be necessary for your legal and regulatory compliance obligations. Proactively engage your legal team to make sure you understand your regulatory obligations in different jurisdictions, particularly if you are a multinational company.

Also, you may consider building a relationship with your regulators. Sometimes it's the regulators who have an advanced understanding of the threat landscape, which could help you prepare for what's coming. Don't assume that if data wasn't stolen, regulators aren't that interested. They are constantly on the lookout for new threats and exploits. They will probably be interested in what you did about an adversary positioned in your organization with potential access to data, even when there is no evidence that data was taken outside of the organization.

It also gives you a chance to show how you dealt with the threat (e.g., "Well, we took it from that event, and we worked backward, and forward, across the kill chain, to understand what could have happened, and what has happened."), which helps regulators get a better understanding of the robustness of your processes and programs, which could make future dealings smoother.

1. https://www.paloaltonetworks.com/engage/communicate-cybersecurity-risks-with-your-board/reply-to-regulatory-inquiries
2. https://www.paloaltonetworks.com/engage/answering-top-board-questions-about-cybersecurity-risks/unit42-retainer
3. https://www.paloaltonetworks.com/unit42/respond/incident-response

LeeAnne Pelzer is a consulting director of Unit 42 at Palo Alto Networks



An Antidote to Stress in Cybersecurity

By Gemma Garcia Godall

Stress is an unfortunate, but unavoidable occupational hazard in cybersecurity. Think about it. Each time you go to work—or, in today's world, log on from home—you are facing thousands if not millions of potential attacks. If a single one is successful, it can cripple the business and leave permanent scars on your organization's credibility and goodwill. It can damage your own reputation and job security.

Whether you are the chief information security officer (CISO) at the top, or an analyst working in the security operations center (SOC), the cumulative effects of constant stress can feel overwhelming. And that's just in normal times.

When your organization has been breached, the pressure ratchets up intensely, to the point where many cybersecurity leaders and professionals feel they can never log off. They risk the anxiety of being in reaction mode all the time, 24 hours a day, seven days a week, often for weeks or even months at a time.

The shift to work at home for employees and IT teams as a result of COVID has piled even more challenges on cybersecurity teams that were already typically short-staffed, and operating beyond their normal capacity. It is a vast understatement to point out that dealing with that amount of stress is unhealthy. The statistics offer sobering and scary testament to the emotional impact of stress in cybersecurity.

More than 90% of CISOs said they suffer from moderate to high stress and a third believe their jobs would be at risk if their organizations were breached, according to a survey of 408 CISOs in the U.S. and U.K. Even more worrisome: 26.5% said stress was impacting their mental or physical health; 23% said the job was eroding their personal relationships, and 17% said they turned to medication or alcohol to deal with job stress.[1]

This isn't just bad for these individuals and their teams; it's bad for business.

I am not here to tell you that you can eliminate stress from cybersecurity. As I said upfront, stress is an unavoidable occupational hazard. But I am here to tell you there is a proven way to deal with stress, and alleviate the pressure so teams can work productively and collaboratively even under the most trying of circumstances.

Managing stress effectively in cybersecurity starts with focusing on emotional intelligence (EQ) and, subsequently, practicing intelligent emotional leadership. Frankly, I shudder with trepidation as I write these words. It is my experience that many hard-driving business leaders, and computer professionals, are wary of the word "emotional." It is also my experience that this happens more often with men than women.

If you've gotten this far, I urge you to continue. If you take in even a little bit of what I have to share, it will help – and may even reshape some of your attitudes at a time when organizations are desperately craving leaders who can think creatively, innovatively, and empathically. When we can include emotions balanced with our rational thinking, we are more successful and happy. When we are authentic to ourselves and our colleagues, we build closer and more powerful teams.

Transformative Power

I've come to believe in the transformative power of EQ and emotional leadership from two vantage points. First is the scientific evidence of its benefits; second is personal experience.

Let's start with science. In the digital age, it is a natural tendency to rely primarily on data, facts and rational thought. However, we can never forget the human element, particularly in cybersecurity. Even with artificial intelligence and machine learning, many critical decisions will be made by humans, and everything that is impacted by people will have an emotional layer. »

Scientists at UCLA[2] have demonstrated that expressing emotions reduces the emotional reaction in the amygdala, which is the component in the limbic system that is best known in the processing of fear. When we are exposed to a fearful stimulus, information about that stimulus is immediately sent to the amygdala, which then sends signals to the brain to trigger a reactive response, such as "fight, flight or freeze."

Research suggests that information about potentially frightening things can reach the amygdala before we are consciously aware, meaning a fear reaction may be initiated before we even have time to think about what might be so frightening. The scientists at UCLA have proven that putting feelings into words is a positive way to reduce the pressure on the amygdala. So, I always encourage all leaders to speak about their own fears in a trust environment to avoid reactive responses.

Now the personal. I was one of those hard-charging business executives I mentioned earlier. I wasn't in cybersecurity, but I was the CEO of a mid-sized company. I worked insane hours, weekends, nights, constantly on the phone, online, on high alert, "on" all the time. I felt it in my body, pressure in my chest. My doctor warned I was headed for a stroke, or heart attack. I needed to stop, relax. But I couldn't. I refused to listen to my doctor, or my body. I had headaches every day, constant pain in my chest.

My breaking point came when I saw myself through the eyes of my 8-year-old daughter. I promised her that I would spend more time with her and her younger brother, and spend less time at work. "Mommy, I don't believe you," she replied, angrily. "You always say you are going to work less and you never do it. And the worst thing is, you are not okay. I can see it in your eyes."

This was a real turning point for me. I realized she was right: I was not okay at all. So I changed. I decided to get a coach to guide me to become aware of my emotions, accept, and manage them. I learned to share them with people I trusted. I learned that being open and vulnerable sometimes makes me stronger. I eventually left that job, and I am now devoted to training business and technical leaders on the value of EQ and emotional leadership. As I've experienced firsthand, emotional leadership can not only change your relationship with your teams and colleagues; it can also change your life.

Understanding Emotional Leadership Competencies

Everything we say, and do, is affected by our rational intelligence – but also our feelings. Emotions have an inevitable effect on all of our activity, and even more so if we are a leader. In leadership, it is commonly accepted that interpersonal skills matter more than cognitive skills. Examples of interpersonal skills include, the ability to communicate; show respect; express empathy; active listening; adapting to your environment; giving, and receiving feedback. These are all competencies of emotional intelligence.

Because interpersonal skills are key to communicating and managing our relationships, EQ is a must for today's digital leader. But what does EQ actually mean? I use this simple definition: ***Emotional intelligence means being able to identify, understand and manage our own emotions and also the same applied to others' emotions.***

To be able to connect with the emotions of other peoples' we first need to be able to identify, accept and manage our own emotions. The leader that reacts to pressure with angry screaming, who loses control and shows low capability to manage his or her own emotions, will have serious difficulties connecting, understanding and managing emotions in others.

In a stressful cybersecurity environment, the results of this type of leadership can be disastrous. Emotions are highly contagious. If the leader reacts poorly to stress, the team reacts poorly to stress. In the work I do, with CEOs all around the world, I see leaders who have what I call "emotional radar" and others who do not. To develop emotional radar and be able to perceive the emotions of those around you, you need to be in a state of internal calm. Without our own self balance, the emotional radar will never work.

Each of us has at least three types of intelligence: rational, emotional and intuitive. When a leader is emotionally intelligent, I say he or she is a balanced leader who has the ability to include and balance these three types of intelligence.

How to Lead with Emotional Intelligence

Talented people – particularly younger people – love this kind of leader. The next generation of people with high technical skills wants to be led with empathy and autonomy. In cybersecurity, where the skills shortage is pronounced and competition is fierce to hire, retain and inspire talent, the difference in leadership can have long-term tangible benefits; and the risk of poor leadership can likewise have severe negative consequences.

As Fred Laloux wrote in his book Reinventing Organizations, the future will no longer be organized as in the Industrial Era, where the boss gave instructions and humans worked as machines. Modern organizations are more refined; decisions are made based on trust and collaboration instead of on ego-driven fears, ambitions and desires. On the current VUCA world, where we need to face Volatility, Uncertainty, Complexity and Ambiguity all together, there is no super leader who has the capacity to decide on his own and find the way alone. Team power is vital, collaboration is essential to generate Collective Intelligence and overcome the challenges. So the leader needs to have EQ to generate the right environment for the team. »

Today's Talent Wants to Be Treated as Human Beings. Are You Ready for That?

Based on my experience working with dozens of leaders and teams, I have several practical recommendations on how to leverage emotional leadership to effectively manage cybersecurity teams in today's environment – particularly in light of the uncertainty and disruption that has been caused by COVID.

- **Breathe**: Whenever you feel triggered by emotions, just stop six seconds and breathe. Take one to three deep breaths. Our breathing connects us immediately with our body and has the key to connect emotions with our rational thinking.
- **Sharing**: Working from home means we all have to share a little bit more of our private lives with our colleagues. This should be a good thing. I've heard leaders say that they have two separate lives, their work life and then their personal life. But that is not the real world. Each of us is one whole person, we cannot be split into two. We need to integrate both parts. We need to feel warmth and be authentic. It is important to be open, to talk about our personal ups and downs, and also our fears, concerns, triumphs and losses. As the leader, create the space and trust for sharing, ask your team directly: What is the worst-case scenario? As I said before, iIf we speak about our fears we can confront them. We can put light on the darkness.
- **Meetings**: Build into the work process informal spaces to connect. With people working from home, we run the risk of losing some of that personal connection that takes place in an office, at the coffee machine or during lunch breaks. Put aside 40 minutes each week where you have a team call where you don't talk business, you just connect as human beings. Also, when you are conducting work meetings, create a space at the beginning and the end to talk. Check in as the meeting starts: How are you feeling today? Are you ready to address today's challenges? Is there anything worrying you? Check out before the meeting ends: What did you think of the meeting? ArE you prepared to take the next step?? Create the emotional energy for the team to work at their best.
- **Feedback**: This is a vital point for any team going through a crisis such as a cybersecurity breach. Every tech professional nowadays needs to learn and improve continuously to deal with today's rapidly changing environment. Talented professionals may be highly prepared for their jobs, but face new challenges they have never before confronted. How can they evolve if they don't receive quality feedback? So prepare your team for that.

One of the keys to being an emotionally intelligent leader is the ability to give and receive feedback. Feedback triggers emotions, so it is important to pay attention to the emotional impact feedback may have on you and others. Feedback needs to be:

- Constant and integrated as a process for improving and learning.
- Bidirectional – it is just as effective to give as to receive.
- More positive than negative. A Harvard study talks about a ratio of feedback/performance in a work team, i.e., leaders should give six positive comments for each negative comment in order to keep people motivated.

Here is an effective formula in having a positive feedback conversation:

- Prepare the environment, the right place, the right time.
- Explain the situation (facts as specific as possible).
- Explain the behaviour seen.
- Explain the impact of the behavior.
- Make your suggestion.
- Encourage the person to do it better the next time and focus on future possibilities.

Always check how the message has been received. How do you see it? Can we agree on my suggestion? Any alternatives? Assertive communications is a key skill for the emotional leader. Practice it.

As you would learn a new programming language, or sign language, or any other new form of communication, get ready to understand emotional language, I can tell you it is much easier than all the technological or business knowledge you have learned. You only need to put a little bit of attention to it and ask for training if needed. You will be surprised at the amazing results you will get with relatively little, but focused, effort.

Being Flexible

COVID-19 has taught us that organizations need to be flexible to succeed in today's environment. We are not machines – why do we continue working as if we were? Taking care of our human part increases our productivity. For example, we don't need to all take breaks at the same time or eat at the same time. Some people work better in the morning, others at night.

Young professionals understand that flexibility and autonomy lead to more productive and empathetic corporate cultures. I know of one company where many of the employees love surfing, the water kind not the web kind. On rainy, dark days their part of the office is bustling and amazing work gets done. On windy days, not so much. The result? High engagement and rotation near to zero on fintech. So apply your own formula and be creative!

The Best Leaders

To me the best leader is the one that role models what we want to see on the team. Leaders can be a role model by using mistakes to teach, sharing emotions but also learnings and challenges, »

offering help and care to colleagues and team members to find better solutions and become stronger.

We are never going to eliminate stress from cybersecurity unless we eliminate the human element, and it would be a sad day, indeed, if that were to ever happen. For the foreseeable future, at least, people will remain vital to successfully navigating the digital age. And as long as we are managing people, we need to be able to manage their stress.

Good leaders understand the value of emotional intelligence in inspiring, motivating and empowering today's workforce. As the workplace continues to change in response to a global pandemic, good leadership in cybersecurity may mean the difference between avoiding breaches and protecting the organization or, at the other end, being more vulnerable to successful attacks.

In today's era, cybersecurity leaders can't afford to ignore emotions and the power of intelligent emotional leadership. Emotions are part of our whole intelligence. In fact, I can assure you that the best leaders will be the ones that embrace and harness it.

As a computer needs electricity to work, we need emotions to give us energy. Emotions are the energy that moves us into action. Emotions move teams to do amazing things. Emotions move the whole world.

This article is excerpted from Godall's chapter in the book **Navigating the Digital Age, The Definitive Cybersecurity Guide for Directors and Officers, Third Edition**. *We invite you to download your free digital copy.*[3]

1. *Life Inside the Perimeter: Understanding the Modern CISO*, Nominet, February 14, 2019.
2. "Putting Feelings Into Words: Affect Labeling Disrupts Amygdala Activity in Response to Stimuli," Psychological Science, May 2007.
3. https://start.paloaltonetworks.com/navigating-the-digital-age-fy22.html

Gemma Garcia Godall is the founder of Instituto de Inteligencia Emocional

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).

The Machines Are Coming: Financial Services Can Reduce the Blast Surface with Zero Trust

By Tarun Khandelwal

We've all seen movies and TV shows where SWAT teams or military forces take heroic steps to safeguard lives and property in the event of a bomb threat. Chief among the defensive efforts they put in place are ways to reduce the impact of a potential explosion—reducing the blast surface. Often, they use machines such as remote-controlled robots to safeguard their human team members. Obviously, they want to prevent the blast from happening in the first place, but at the very least, they want to ensure they can mitigate its impact as much as possible.

The same approach holds true for thwarting cybersecurity attacks, particularly in the "target-rich" financial services industry. Although financial services firms have often been in the forefront of adopting cybersecurity tools, technologies and processes because of the nature of their industry—after all, it's where the money is—more needs to be done. The bad guys are relentless, while also increasingly sophisticated in their attacks.

This has put intensified pressure on the financial industry to not just adopt a Zero Trust model of cybersecurity protection, but to aggressively embrace the ideals of Zero Trust: Trust nothing and no one, log everything, and invest heavily to validate users and machines.

A Ripe Target

It may seem obvious to those of us in this vertical market, but it bears repeating: The financial services sector may be the single-most-targeted industry for cyberattacks. A recent headline from an IDC report stated it bluntly: **The financial industry is more susceptible to IS infrastructure security breaches than other industries**.[1]

The IDC data is stark: 96% of IT and security professionals said their organization has been attacked by viruses, and the financial industry is 50% more likely to be targeted for unauthorized-use attacks than are organizations in all other industries. The IDC analyst authoring the report said it well: "For these (financial services) companies, security is not a value-added feature. It's a core requirement for conducting business." »

While the financial services industry has always been an attractive target for hackers, the impact of how work has changed during COVID-19 has raised the stakes even higher. Research done with UK-based IT and security professionals points out that most believe COVID-induced work-from-home practices and remote work are accelerating attack risks in the financial services industry.[2]

I'm sure no one was surprised by these revelations, given the attractiveness of financial services data, such as customer records and personally identifiable information...let alone the ability to actually steal money and other financial assets. Many of us also know that cyberthieves are using "machines" to do their dirty work, such as automated attack tools, as well as artificial intelligence and machine learning algorithms.

Another challenge is that our industry has an increased use of what I call "ephemeral computing," such as cloud services and on-demand technology services. While cloud is arguably more secure than any single organization's data centre, misconfigurations and oversight can leave an organization's crown jewel data exposed in public, as we've seen with an increased number of highly public stories. Many organizations still apply manual procedures to highly automated ephemeral technology.

Using Zero Trust to Reduce Your Blast Surface

Undoubtedly, all CISOs reading this article, as well as nearly all business leaders and board members, are well aware of the importance of Zero Trust. By starting with an assumption that we must view any attempt to access information with suspicion and whose credentials must be validated, we take the first step toward reducing the blast surface.

But in order to fully exploit the benefits of a Zero Trust framework, financial services organizations need to keep in mind that Zero Trust is not an event—it's a journey. You must start with an initial step, and proceed with painstaking discipline and a willingness to abide by the key principles of Zero Trust.

Specifically, financial services companies must:

- **Trust nothing and no one**. Even something as simple as logging onto the network must be treated with suspicion and a wary eye. That's why multifactor authentication must be a starting point for a Zero Trust philosophy, and should become increasingly sophisticated through the use of such techniques as biometric authentication and frequent password changes.
- **Log everything**. If you accept the assumption that hackers will occasionally succeed at getting through your initial defenses, you must have a timely, accurate and complete record of all login attacks, user behavior and data movement.
- **Invest aggressively in tools, technologies and practices that validate both users and machines**. Not only are the hackers getting smarter in hiding their own identities by simulating those of authorized users, they also are hiding the true nature of their machines. As I mentioned earlier, they are becoming prime users of automated tools and algorithms to expand their ability to compromise systems and exfiltrate data.

Security Is Everyone's Business—but Someone Has to Take the Lead

One of the key elements of Zero Trust is that it's not just the responsibility of the information security and IT teams to implement, manage and review. The entire organization must have a Zero Trust commitment, especially in the financial services sector where we have so many touchpoints, and the regulatory, legal, operational and brand risks of messing up can be devastating.

In fact, Zero Trust is so essential to a successful cybersecurity defense in financial services that CEOs, CFOs and other non-technical C-suite executives must set the right example. The risk management team alone can't do it because they are often seen as the "office of No," often viewed with scorn by many rank-and-file employees. Leadership must accept ownership of Zero Trust, and must endorse full-bodied investment in Zero Trust tools, technologies, services and processes. Business executives sponsoring new initiatives can protect their larger organizations by inspecting and insisting on allocating sufficient funding to go towards information security as part of the initiative.

It's also important for leadership to be willing to commit to investments in security automation (our own machines) to combat the smart tools used by hackers. That's because we, as an industry, still rely too much on manual, human-powered processes. Even though our organizations all benefit from having smart, hard-working and dedicated professionals watching out for our cybersecurity, that's not a match for the machine-centric approach cyberthieves are taking.

We have to use machines to do more real-time work, such as event analysis and remediation or studying anomalous network and user behavior. In essence, we must use machines to fight the other guys' machines, or we risk falling into a very bad position—playing catch-up when every second counts. The more manual your approach is to cybersecurity, the more at risk you are. This is an important precept of Zero Trust, as well: automate as much as possible to limit the impact if and when a breach occurs.

I don't want to kid anyone. Zero Trust, alone, won't prevent financial services organizations from being breached. You do need to invest not only in powerful technology tools, subscription services and human expertise, but also in smart processes. Adopting a Zero Trust mindset, and the discipline and hygiene that go along with it, will better protect your organization by dramatically reducing the blast surface.

1. Frank Dickson and Christopher Kissel, *IDC 2021 Ransomware Study*, IDC, July 2021.
2. Phil Muncaster, "Most Financial Services Have Suffered COVID-Linked Cyber-Attacks," Infosecurity, January 19, 2021.

Tarun Khandelwal is an executive security advisor to the financial services industry and the former head of security architecture at CIBC

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).

IoT Adoption in Healthcare Brings Security Opportunities

By Anand Oswal

Connected medical devices, also known as the Internet of Medical Things or IoMT, are revolutionizing healthcare, not only from an operational standpoint but related to patient care. In hospital and healthcare settings around the world, connected medical devices support critical patient care delivery and a wide variety of clinical functions, from medical infusion pumps and surgical robots to vital sign monitors, ambulance equipment, and so much more. At the end of the day, it's all about patient outcomes and how to improve the delivery of care, so this kind of IoT adoption in healthcare brings opportunities that can be life-changing, as well as simply being operationally sound.

Yet, enabling these amazing patient outcomes through IoT technology brings with it an associated set of security risks to hospitals and patients that are in the news far too often. Ransomware, for example, is a particularly prevalent threat to healthcare providers around the world. In August 2022, the French hospital Centre Hospitalier Sud Francilien (CHSF) was the victim of a ransomware attack that disabled medical imaging and patient admission systems. And in October 2022, CISA issued an advisory to healthcare providers warning of a ransomware and data extortion group targeting the healthcare and public health sector with a particular interest in accessing database, imaging, and diagnostics systems within networks.[1] But ransomware isn't the only risk. In fact, according to a report in HIPAA Journal, there has been a 60% increase in cyberattacks of all varieties in healthcare in 2022,[2] making it an unfortunately routine aspect of delivering care that the industry must be prepared to address.

Why Medical IoT Devices Are at Risk

There are a number of reasons why medical IoT devices are at risk. Among the most common reasons is the fact that many of these devices are not designed with security in mind.

Many connected devices ship with inherent vulnerabilities. For example, according to research from Unit 42, 75% of infusion pumps have unpatched vulnerabilities.[3] Over half (51%) of all X-Ray machines had a high severity CVE (CVE-2019-11687), with around 20% running an unsupported version of Windows.[4]

Unit 42 research also found that 83% of ultrasound, MRI, and CT scanners run on an end-of-life operating system.[5] Those operating systems have known vulnerabilities that can potentially be exploited. Attackers are known to target vulnerable devices and then move laterally across the organization's network to infect and damage the rest of a hospital network.

The impact of medical IoT device vulnerabilities is serious and potentially life-threatening. It's not always easy and sometimes not even possible to update or patch some of these devices, either because doing so requires operational disruption of care delivery or due to a lack of computing capability of many types of devices. As a result, we've seen patient data exposed. We've »

seen hospital operations halted. While the attack potential is widespread, healthcare providers can take proactive steps to help minimize the vast majority of device-related security risks.

Four Necessary Steps to Improve Medical IoT Security

Among the challenges that medical facilities and health providers face is actually being aware of all the connected devices that are present. Visibility, however, isn't the only thing that is needed to improve medical device security. In fact, there are four steps that can be taken to secure devices and reduce risk:

- **Ensure visibility and risk assessment of all connected medical and operational devices**. The first step in securing IoT in healthcare is to know what's there; you can't secure what you can't see. Device visibility isn't enough—you have to be able to continuously assess the risk the devices and their evolving vulnerabilities pose to the network.
- **Apply contextual network segmentation and least-privileged access controls**. Knowing a device is present is useful. What's more useful is understanding what network resources or information can be accessed by the device. That's where network segmentation comes into play, creating and enforcing policies that limit device access to only the resources necessary for its intended use and nothing more.
- **Continuously monitor device behavior and prevent known and unknown threats**. As these devices communicate across clinical environments and with external networks and services, they ensure that you establish baseline behavior, monitor devices for anomalous behavior, and protect network-connected devices against threats such as malware.
- **Simplify operations**. In order to effectively manage and secure the sheer volume of devices on a healthcare network, providers require a solution that integrates with existing IT and security solutions to eliminate network blind spots, automate workflows, and reduce the burden of tedious manual processes for network administrators.

Better IoT Security Helps Ease Regulatory Compliance Challenges

Understandably, there are a lot of compliance requirements in healthcare. Healthcare compliance covers numerous areas like patient care, managed care contracting, Occupational Safety and Health Administration (OSHA), and Health Insurance Portability and Accountability Act (HIPAA) privacy and security, to name a few. Any attack that involves a patient system or medical IoT device is most likely a compliance breach, resulting in the loss of sensitive data or access to sensitive data from unauthorized entities. Limited IoMT visibility and risk assessment make it difficult to meet regulatory, audit, and HIPAA requirements. Having complete visibility into all devices and their utilization data reduces the burden of preparing for compliance audits and compiling compliance reports.

Implementing Zero Trust for Medical IoT

Humans place their trust in medical professionals to improve and sustain human health. Medical facilities rely on their technology to do the same. But trust should not be granted by default. It needs to be continuously monitored and validated. That's where a Zero Trust approach comes into play.

Zero Trust, in very straightforward terms, is a cybersecurity strategy that seeks to eliminate implicit trust for any user, application, or device accessing an organization's network. Zero Trust is not a product. For many customers, Zero Trust is a journey. For medical IoT security, Zero Trust starts from understanding several key things:

Who is the user of the device?

What is the device?

What is the device supposed to do?

Is the device doing what it is designed for?

On a continuous basis, Zero Trust means monitoring devices and their behavior for threats, malware, and policy violations to help reduce the risk by validating every interaction.

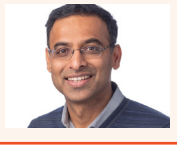
Take the Zero Trust Path of Least Resistance to Improve Healthcare IoT

Healthcare IT and security teams are overburdened, so security implementation shouldn't be onerous. Improving security for medical IoT devices shouldn't require a forklift upgrade of hospital networks either.

Most healthcare providers already have network firewalls that act as enforcement points for Zero Trust device security. When you want to enable visibility, risk assessment, segmentation, least privilege policies, and threat prevention on the journey toward Zero Trust, it should be done with as little friction as possible. Machine learning (ML) can also dramatically accelerate policy configuration, which can be automated. If security becomes another big project that requires significant human effort, it has less chance of being successful. Security needs to be integrated, easy to deploy, and as automated as possible.

Medical IoT devices help to improve human healthcare every day. Just like humans need to do the right things to stay healthy, it's essential for medical IoT devices to remain healthy too. Lives literally depend on it.

1. https://www.cisa.gov/uscert/ncas/alerts/aa22-294a
2. "Healthcare Seeks 60% YoY Increase in Cyberattacks," HIPAA Journal, November 17, 2022, https://www.hipaajournal.com/healthcare-sees-60-yoy-increase-in-cyberattacks/.
3. Aveek Das, "Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization," Unit 42, March 2, 2022, https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/.
4. Jun Du, Derick Liang, Aveek Das, "Windows XP, Server 2003 Source Code Leak Leaves IoT, OT Devices Vulnerable," Unit 42, November 6, 2020, https://unit42.paloaltonetworks.com/windows-xp-server-2003-source-code-leak/.
5. Ibid.



Anand Oswal is senior vice president and GM of Network Security at Palo Alto Networks

Leveraging Cybersecurity to Supercharge Retail's Frontline

By Ravi Balwada

In retail, we don't have the luxury of thinking about security as an afterthought. We have to think about security early in the innovation process and make sure our security best practices, governance and architectures are taken into account when we are designing our solutions—everything from defining what a container needs to look like when we deploy something to what sort of access controls we have.

With modern cybersecurity technology, we have better tools and instrumentation to monitor environments more effectively, to change the security posture very rapidly and meet the changing needs of the company—whether it is adapting to a new wave of mobile devices or introducing a new population of workers to information that is sensitive.

Also thanks to modern cybersecurity, new use cases have become available in retail that were never possible before. Many retail leaders talk about the changes being enabled for their customers, but it's also vital to explore the exciting new ways retailers can enable their frontline workers.

Three areas cybersecurity is helping to supercharge our frontline workforce

When you focus on cybersecurity in an environment like Guitar Center, you have the power to do amazing things—for your sales associates, customers and overall business. Here, digitization and cybersecurity are empowering our sales associates in three major aspects of our business:

- Customer service
- Back-office functions
- Efficient, individualized, business management

Securing a new level of customer service and relationship

Our mission is to build a lifetime relationship with our customers in their musical journeys. Whether it's lessons, product, repair or rental services, acquiring or selling used equipment, technology connects how we build our relationships with customers. Customers can start online and finish in a store; start in a store and finish online; or any combination they choose.

As a result, we're shifting the engagement with the customer to the aisle instead of at the point of sale. In a previous incarnation of our business it was: "What do you need? Let me ring you up." Now we are about: "Let me work with you collaboratively. »

I understand who you are, your needs, your aspirations. Let us brainstorm and together we can find the best solution. Let's move this conversation to the aisle where I can help you make good choices."

Our sales associates leverage information across all channels, which changes the conversations we have with customers. If you're a salesperson, you actually know if the customer has been browsing certain items online. You know what the customer has purchased in the past. You can make recommendations for equipment, lessons, sheet music. You can help them complete their purchase and you can help them take advantage of other things that might make their musical journey more fulfilling.

For our almost 12,000 frontline sales associates, it's no longer a world of Post-it notes and pieces of paper. We are bringing a massive amount of information and insight. They have full visibility into supply chains, status of inventory, deep insights into each customer, and much more. They are dealing with volumes of information around dozens of variables. There is far more data and activity at the edge and a much larger attack surface.

This requires cyber innovation and evolution. You now have multiple places where data is residing that have to be secured, which means you need cybersecurity with visibility and granular access controls to ensure that the right people are accessing the right information at the right time. There is also the challenge of forensics and investigation of security incidents. We need systems that have amazing logging and automation for us to be able to react very rapidly to any security incidents. That requires us to work with modern technologies that are agile and can very quickly be swung into action.

Our data management is a key focus, including building data lakes and visual analytics capabilities that we are introducing across our entire enterprise. We also have to make sure we have a secure platform. We are replatforming our firewalls and leveraging new technology around identifying threat patterns—isolating problems when necessary, isolating our environments so they are more effective. Only through these kinds of moves can we support our associates to build those deep customer relationships that fuel their success.

Supporting the latest back-office functions

Our associates have new frontline tools that enable not only customer relationship management but back-office function. For example, every associate will have a mobile device. If associates need to perform actions such as pick up from a store, ship from a store, or access inventory, they have the information at their fingertips using their mobile devices. This provides a tremendous benefit for each of our people, but it also means our endpoints will increase ten times versus what we have today.

With each new device and endpoint, we put powerful capabilities in the hands of associates. You have to have amazing security—with isolation, compliance, controls, encryption, edge protection, and more. We are giving associates the ability to process payments on mobile devices. As you run financial transactions on mobile devices, on wireless networks, you need to prevent associates from compromising personal identifiable information. Another important factor is the ability to onboard people quickly and efficiently, especially with our seasonal workforce. Technology compresses time to value so they can be productive faster with information that is easily available and tools that are highly intuitive. And this speed only becomes possible when all of those interactions are properly protected.

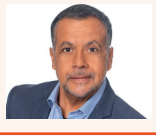
Bringing new levels of management to the business

At a time when retaining and motivating workers is paramount to business success, Guitar Center has been executing operational advancements that are geared toward empowering and engaging our associates in new ways. Today, sales associates can manage their own businesses from their mobile devices. They can view status on commissions; access training; get real-time information on promotions; collaborate with colleagues and peers. It's not enough to just build an application that works on mobile devices. It has to be engaging. We're building experiences across the enterprise that are more gamified.

It is an important, fundamental change—knowing that we have a security posture to support this kind of innovation. We continue to harden our security to ensure all of our 12,000+ sales associates can be more and more digitally enabled.

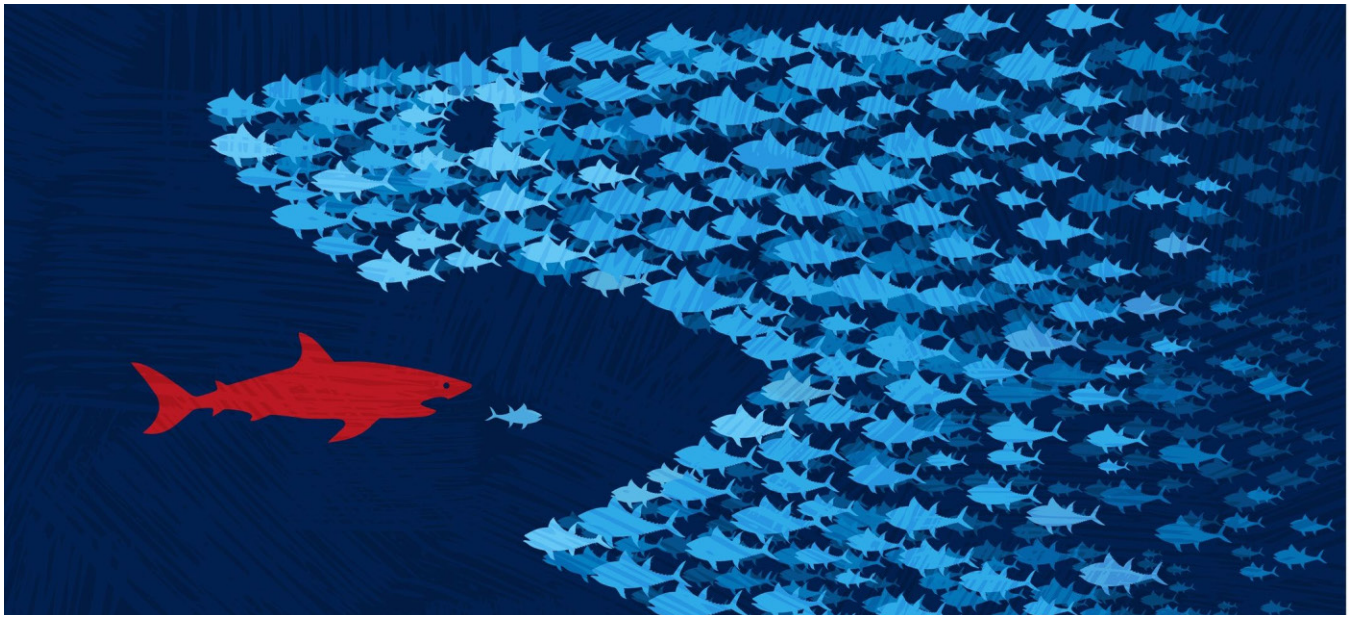
Enabling workforce satisfaction, innovation, and long-term success

The value of empowering sales associates with robust, secure, digital experiences cannot be overstated, especially in today's environment where workers have more options and are seeking jobs that are more enriching and satisfying. There is, however, one caveat. The kind of data-driven frontline innovation I am describing is only possible when we invest in and treat cybersecurity as an enabling technology, and a nice-to-have. At Guitar Center, we are always aware that we can only do the things we want to do if we have the security that we need.



Ravi Balwada is chief technology officer at Guitar Center

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).



Building a Collective Defense: A Strategic Cyber Initiative for Private Sector Leaders

By Ron Banks

Before entering the private sector as a cybersecurity executive, I spent more than 29 years in the military, serving as an officer in the U.S. Air Force. Military strategy was my focus for more than a decade, but I didn't connect it to my interest in the cyber domain until after a revealing conversation with a 4-star general.

The general, who was responsible for the physical defense of the United States, asked me: "Why don't we work well with cyber command? Why don't we have a more holistic strategy to combine the skills and capabilities of kinetic [physical] forces and cyber forces?"

In short, this general had a valid complaint: National cyber strategies were lacking real teeth to properly defend the nation.

While in the military, I received extensive training in formal strategy and led combat operations. I learned important theories behind how and why sound strategy was essential for military advantage. But this conversation was my "aha!" moment where I came to understand the benefit of what I now call *collective defense* as it relates to the virtual domain. During my military career, it meant promoting and enabling collaboration between military and cyber forces of all U.S. government entities—and ensuring the rank-and-file created and carried out a comprehensive strategy. That strategy of collective defense is equally applicable—and maybe even more necessary—in the private sector.

Why the private sector needs a collective defense

As the chief information security officer (CISO) of a financial institution, I am confident that if we encounter a robbery, law enforcement will be there in a heartbeat. But in the virtual domain, that is not the case – we are left to defend our respective firms on our own. In the battle against virtual threats, we witnessed the disintermediation of traditional law enforcement responses to a cybercrime in the private sector. Cyberthreats can engage directly with private corporate networks without law enforcement being able to deter or stop those threats.

Governments and regulatory agencies impose a number of rules and requirements on private sector firms related to their cybersecurity, especially in financial services, but also in an increasing number of markets. Unfortunately, for many of those organizations, cyber regulations are placed on the private sector without government help to defend private companies. Also, when it comes to combating cybercrime, especially those originating overseas, corporations often are left without enough help, or the right kind of help.

For example, private sector companies often receive unclassified information a little too late, or the information is too generalized for CISOs to properly use. As a result, security leaders in the private sector need to look elsewhere to find actionable, timely information. Additionally, law »

enforcement—which today is far more willing and able to take on a cyber investigative role—still struggles to go after criminals because of jurisdictional and capacity hurdles. Occasionally, they may get an indictment, but it rarely seems to lead to extradition, prosecution, and conviction. Therefore, there are very few consequences imposed upon malicious cyber actors, which also accounts for their continued growth in sophistication and competence year after year.

We now see cybercrime has become commoditized. Cyber incursions happen more often than in the past, so much so that it has become "cybercrime as a service." The hackers' bar to entry is very low, leading to more threats and more sophisticated attacks. Clearly, no single corporation—not even large, well-resourced ones—can contend with the sheer scale of today's cybercrime without help from security firms and colleagues in the public sector. *Where can corporations turn?*

Now is the time for leaders to emerge

If private sector organizations hope to have a chance at staying ahead of attackers in today's landscape, a thought leader is needed to serve as a catalyst for action and bring together the private and public sectors to marshal their resources, talents, and experience against the attackers. That leader may be a company in the cybersecurity space, an industry organization, or a government agency. The issue is less about the affiliation of the group or person taking the lead, and more about acting as a galvanizing force for ideas and action.

It will take a leader to sponsor the kinds of blunt conversations required now—ones that put aside blame, focus on the problem, and provide a range of possible solutions. Unless we bring together the right leaders from the private and public sectors to form a framework for collective defense, all of us—the public and private sector alike—will be forced to muddle along with the status quo, which is simply not acceptable.

What a collective defense can accomplish

In our organization, as is the case with countless others, we model collective defense at a micro level by bringing together a group of highly committed cybersecurity professionals and supporting them with budgets and executive sponsorship. We also seek guidance from responsible and committed board members to assemble the right cybersecurity program. It's a good beginning, but unfortunately, we can only go so far when we go it alone.

Building a collective defense answers the challenge of resource and human constraints; we go further when we go together. Through collective defense, we can create the framework and methodology for analyzing threats and developing solutions by surfacing and sharing relevant, contextualized, real-time information. In a collective defense we are aided tremendously by the fact that we all collect more security information than ever. In fact, there are numerous security giants on the private side that have a unique view into what's happening across the cyberthreat landscape. Many large cybersecurity organizations can see in real time across numerous private firms as cyber campaigns propagate. Working together with one goal in mind—providing better security for our industry—enables public sector entities, financial services companies, and technology leaders to provide collective, proactive steps to spot and defend against an ever-growing litany of threats.

In a collective defense, many firms can share threat information, indicators of compromise/attack, and tactics in near-real time to quickly harden their respective defenses against emerging cyberthreats. Unlike existing threat-sharing organizations that pass overly generalized information too late, collective defenses work together to actively defend against an ongoing attack. Collective defenses are active partnerships to help each other understand and defend against the cyberthreat in real time.

Overcoming barriers to building a collective defense

In the financial services sector, we've started to see some early work on building a collective defense, as has been the case in other industries. But none of this action has scaled yet. That's the key, and admittedly, it's a tough thing to do.

In the private sector, we're understandably zealous about trying to protect our competitive edge, and we often have an innate fear of sharing information with our competitors. The cyberthreat is one we all have to battle. We must make companies comfortable enough to be part of this collective and to enthusiastically participate in this collaborative problem-solving. There also are legal and regulatory challenges in bringing together industry players—some of whom may not always be comfortable sharing information. Collective defenses would not have their regulatory agencies in the room, and there must be an agreement that any activities or information sharing between participating firms would not be passed to regulators.

That's where the thought leader I mentioned comes in. A strong leader, or a few leaders, need to step forward with the clout and confidence to cajole and reason with people till they are comfortable being honest and open in sharing information about what they're seeing, what they've seen work, and what they've learned doesn't work.

Some companies have hesitated to step into that leadership void, saying they believe it's the U.S. government's role to do that. Regardless of what you may believe, it doesn't absolve us in the private sector from stepping forward anyway; our cybersecurity defenses need more fortification than ever before.

Taking the first steps to build a collective defense

How does a company get started in order to be part of a collective defense? Here are four concrete actions to advance your cause. »

First, obtain your executive leadership and board's backing. They are not only providing strategic vision and insight, but they ultimately give the thumbs-up or thumbs-down to external engagements and spending initiatives.

Second, examine your lineup of technology providers and identify the one or two that are truly partners, offering ideas and sharing best practices rather than just putting a purchase order in front of you to sign. Your major cybersecurity providers have a wide view of cyberthreats across their technology and the firms they support. Consequently, they are a major asset in the collective.

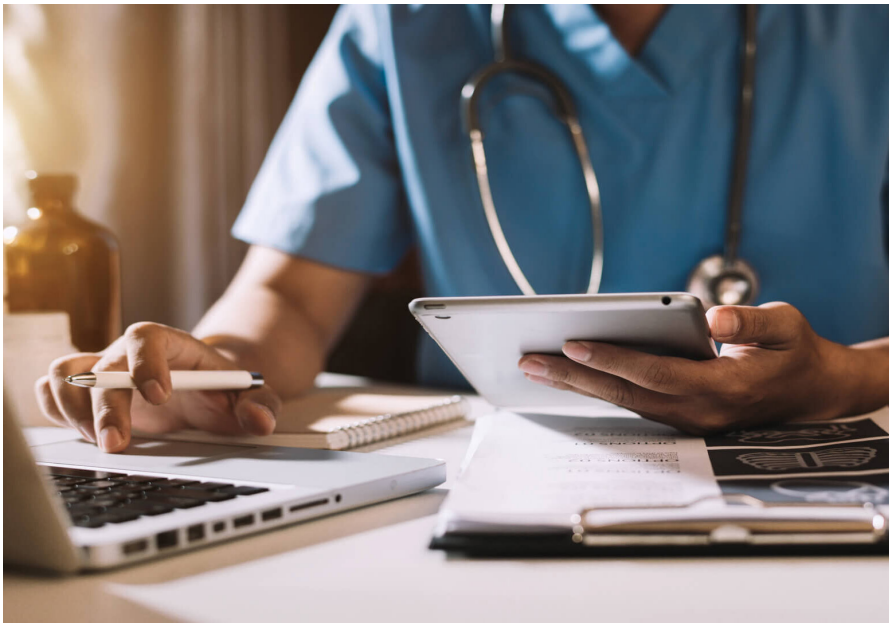
Third, talk to your colleagues at other major companies in your sector. I believe they will embrace this concept of collective defense and join in. Their participation will swell your group's size and influence—remember, there's strength in numbers. Your firm may not be the first to see the emerging cyberattack, but others in your collective might. The greater the number of participating firms, the greater the number of "sensors" the collective has to alert of a new, propagating attack.

Finally, don't overlook the smaller players in your market. Get the word out to them about collective defense, and how it allows smaller organizations with fewer resources to become much more efficient with their own cyber defenses. A smaller partner in the collective will greatly appreciate the type of threat information that can help them to prioritize their defensive actions.

In the end, you'll all be part of an important conversation on the growing cyberthreats we all face. But even more importantly, you'll be doing something tangible about combating them.

Ron Banks is chief information security officer at Texas Capital Bank

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).



Telemedicine Is Surging, but What About Security?

By Jamison Utter

Naturally, the COVID-19 pandemic has put a spotlight on our health care system, the needs of hospitals and doctors, and the care of patients. Although questions about health care inevitably spark spirited public policy debates, there is widespread agreement on the two major factors that get in the way of achieving our goal of better, more efficient health care delivery. One, of course, is cost, and I think it's safe to say we're not going to address that here.

The other one is manpower. What, you may ask, does cybersecurity strategy have to do with addressing the large and growing gap in health care providers for our societies?[1] In a word: Telemedicine.

Telemedicine is a game-changer. It allows our already-stretched legions of doctors and nurses to "see," diagnose and treat patients in a digital environment, rather than forcing a patient to come into a physical office, clinic or emergency room. And while in-person care is obviously essential for many health issues, telemedicine is ideal for many other scenarios.

Maybe a harried parent can't take her sick child to an emergency room. Maybe you have a chronic condition that needs close monitoring, but you don't need to go to a doctor's office every month. I regularly use an oximeter and blood pressure cuff, and my data is safely and securely streamed to my doctor for evaluation and, if necessary, action.

This not only benefits the patients, but also the practitioners and their business organization. Whether health professionals work for a large hospital or a small private practice, telemedicine allows them to help more patients within a given timeframe, while being freed up to devote more in-person time for problematic cases that require face-to-face interaction.

Telemedicine is getting popular, especially as the health care industry is forced to adapt to remote work. »

In New York, the Hospital for Special Surgery[2]—widely acclaimed as a leading orthopedic surgery center in the world—transitioned the vast majority of its 400 doctors and nurses onto a telemedicine platform within days of ceasing all elective surgeries. And in the United Kingdom, the health care system went from handling fewer than 1% of appointments via a video link to a scenario where 100% of doctor assessments took place by phone.[3]

Of course, telemedicine is not new. Much of the dramatic uptake in telemedicine adoption can easily be attributed to the pandemic. But don't make the mistake in thinking this is a temporary development: This is the beginning of a new normal for health care delivery. This is not a stop-gap for the next year or two; it is a permanent shift.

Which brings us to a critical point: Cybersecurity in a telemedicine environment. There are a few key considerations that health care leaders must pay attention to.

Devices

For health care industry administrators, chief medical officers, chief information security officers and tech-savvy practitioners undoubtedly centers on the devices. After all, many doctors and nurses working remotely are likely accessing telehealth applications and patients' health care data through personal devices, home networks and personal cloud services. It's impossible to expect every health care professional to always follow responsible cybersecurity hygiene. Without an on-site security or IT professional, medical professionals working from home must take extra care to ensure that their devices have the proper security controls, identity authentication and security patches.

Data

But the cybersecurity issues go beyond devices. While we all may worry that we are being eavesdropped upon, the bigger issue is the data itself. Yes, it's true that hackers will try to exploit any weakness in the security chain by listening to conversations, but we should be much more concerned with the data. For hackers, medical records are tasty.

Connection

However, the biggest concern is that medical professionals are pushing data from devices over networks to data centers and to the cloud. Vital signs, insurance information, identities—all of these are prime targets for hackers.

Dark Web

There is also a lot of dark web behavior to account for. Think about your own consumer online browsing and buying experiences. For instance, if I go to Amazon and buy a tent to go camping, the next thing I know, I'm being served camping-related ads from Facebook and Google. That unwanted inundation could easily take place in health care, and from less-than-reputable sources. It may be annoying to be served with ads for quack remedies and fake cures, but think about what happens when your spouse starts receiving ads for life insurance after you have received a tele-diagnosis of acute heart disease that you have not yet disclosed.

Patients Have to Be Secured

Fortunately, while these are legitimate concerns, the current state of cybersecurity for telemedicine applications is solid, and it will get even better as adoption spreads. It comes down to thinking through all potential weak points in the telemedicine workflow for protected health information (PHI) data. This must include making well-thought-out choices on who should have access to that data.

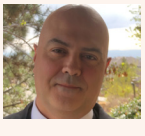
First, make sure you know what the organization is doing to ensure that its systems, workflows and devices are not the weak link. While you can't control everything (like the security settings on a doctor's Android device), you can understand where data is coming from, where it is going, and how it is behaving from the device to the network to the cloud to the data center.

Second, you may want to think about partnering with device manufacturers on improved telemedicine security controls and protocols. I'm not just talking about well-known computing endpoints like notebooks, tablets and smartphones. Think about "smart" Internet of Things devices like dialysis machines, heart monitors and pacemakers. If you have the right ecosystem, it will be a lot easier for practitioners to embrace the technology and use it responsibly.

Everyone must keep in mind that if the patient is not safe—or does not feel secure—you're going to have bigger problems than cleaning up a data breach or dealing with a compliance audit. You'll be facing a crisis of confidence by the very patients that telemedicine is designed to help.

Good luck, and please be safe.

1. Joyce Frieden, "COVID-19 Is Making the Physician Shortage Worse, Groups Say," MedPage Today, March 27, 2020.
2. hss.edu.
3. Agrawal et. al, "To emerge stronger from the COVID-19 crisis, companies should start reskilling their workforces now," McKinsey & Company, May 2020.



Jamison Utter is a security enthusiast working in physical and cybersecurity his entire career

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).

Making Cybersecurity the Smart Investment in an Era of Economic Uncertainty

By Matt Gyde

For business leaders, the time since the outbreak of COVID-19 has been a brutally tough challenge, with no easy calls—just sober, analytical thinking that often results in no one being satisfied, and a nagging fear that you just haven't done enough. I'm not here to tell you it's going to get any easier. But what I'm going to try to do is help you retain a reasonable level of cybersecurity spending. I also want to give you some rationale on how chief information security officers (CISOs) should make their case in the C-suite or the boardroom, and why business leaders should get out in front of this.

What Have We Learned? Plenty

On a personal level, most of us know someone who has been directly affected by the pandemic. For organizations, many are faced with declining revenues and profits, workforce furloughs, customer upheaval, project delays, supply chain disruptions and more.

Our dealings with the pandemic have, however, taught us a few things. First, work from home is not a fad or a short-term accommodation; it is the way more and more people will work in the future. Second, there are very important security implications to work from home, and these are going to entail conversations about budgets and resources. And third, those conversations are not going to be easy ones. Not for cybersecurity executives, CEOs, board members or chief finance officers (CFOs)—not when so many organizations' business opportunities have been severely constrained, or in many cases see their businesses hanging by a thread.

The good news is that we are seeing indications that organizations seem to understand the increasingly strategic role of cybersecurity in this era of the so-called "New Normal." Since the pandemic erupted, I have not had a single executive tell me that their organization's cybersecurity budget has been cut. Although, I assume that people are being honest with me, I'm not naïve enough to think that apparent commitment to holding the line on cybersecurity budget cuts will hold unless a few important steps take place.

Let's Talk: The Right Way and the Wrong Way

Anyone reading is aware that cybersecurity investments must be meaningful, have executive support up to and including the board, and be tightly aligned with business goals. Frankly, those are table stakes. And the stakes just got a lot higher. In order to keep our organizations, our employees, our customers' data and our most valuable digital assets secure, we must rethink the way we all talk about cybersecurity. That's because without the right conversations, CISOs, CEOs, and board members will struggle to find the optimal spending levels that straddle the line between fiscal responsibility and optimizing security as a business enabler.

After having conversations with hundreds of CISOs and business executives about the disruptions this year, I've learned valuable lessons about the right and wrong way for those groups to talk to each other about security spending:

First, the wrong way: Talking about doom and gloom, FUD (fear, uncertainty and doubt) and avoiding disaster caused by draconian cuts to the cybersecurity budget. Board members and CEOs occasionally take a perverse interest in the data breach stories of their competitors and in other industries, and CISOs often fan the flames of those fears in hopes of landing more funding. But those talks rarely, if ever, result in maintaining necessary spending levels for cybersecurity. That's because cybersecurity is cast as insurance, as disaster avoidance, as a moat around the castle keeping out the bad guys. That's a mindset that is still too prevalent in many business meetings, and it marginalizes both the cybersecurity function and the role of the CISO.

Then, there's the right way: Talking about cybersecurity as not just a technology—but as a business enabler. When it comes to cybersecurity budget and cost reduction, engagement must happen at inception. Making security an after- »

thought, after products or services are rolled out, or equating it with insurance, actually costs money...and not just in the long run. Fixing security issues that arise late in the process, because that team wasn't clued in earlier, often results in quick fixes designed to address only the most essential potential glitches in order not to hold up new releases. You have to demonstrate the strong value of cybersecurity to the business, rather than treat it as piecemeal solutions where costs add up. This is especially effective when you are able to measure cyber risk. I would urge all CISOs to read Richard Seiersen's article which gives clear examples on how to achieve this.[1]

Is Cybersecurity Your "No Team" or "Yes Team"?

When your organization fails to include the CISO and their team in the loop from the very start of business conversations, you put them in an unenviable spot: You make them the "No Team." And I don't know of many people who relish being on the "No Team":

- No, you can't let employees use their same passwords at home as they use at work.
- No, you can't extend access privileges to part-time workers.
- No, you can't release the new smart-home product because the security footprint is too big for that sensor.

Instead, think of how to position cybersecurity as the "Yes Team." Think of the sense of empowerment to your business when the team adds value to the business, and makes it more agile:

- Yes, you can expand work from home policies to all employees.
- Yes, you can enable customer self-service on account transfers from mobile devices.
- Yes, you can roll out that sensor-based inventory management system.

Whether the CISO and their team is positioned and acts as the "No" or "Yes Team" depends upon a lot of factors. These include the relationship the CISO enjoys with the CEO and the board, the trust developed among the parties, the extent to which the CISO takes a business view of issues rather than a technology-centric perspective, and many more.

But if the CISO has the foresight, discipline and cultural awareness (read: political savvy) to be an enabler, a problem-solver, a facilitator and a business visionary, he or she will take the key step toward building the perception of their organization as being the "Yes Team." And when you become a "Yes Team," your budget discussions become a lot more strategic, and a lot more fruitful.

Of course, becoming a "Yes Team" is a lot easier when the technology teams and the business units rally around a common goal—or, in this case, a common enemy—to support a more digitally secure organization. Take the WFM paradigm. People had been working from home to varying degrees for a while, but COVID made that the new reality. And what we all found out very fast is that WFM could become a snake pit for employees, suppliers, partners and contractors if the right cybersecurity frameworks were not in place.

The same thing has become evident in cloud services, which are experiencing stratospheric growth across the board in businesses—including, interestingly enough, the development, deployment and support for cybersecurity services. The cloud's potential for delivering cybersecurity has been understood for some time, and now it is becoming a reality. COVID may have accelerated these trends, but the collaboration throughout the organization in response to the pandemic has helped remake cybersecurity into the "Yes Team."

Changing Rules, Changing Roles

For all of us, our organizational roles and priorities have undoubtedly evolved as the pandemic has lingered and its impact expanded and deepened. Take the CISO, for instance. With security budgets increasingly moving away from the centralized control of the CISO and residing at least in part now with business units, CISOs have been moving to build tighter relationships with business executives for some time. COVID has accelerated that to the points where the CISO now is acting more as a trusted advisor to the business.

The CEO, of course, still is singularly focused on big-picture issues and strategy. But now corporate strategy necessarily includes cybersecurity, done in concert with the CISO and others. CEOs have had to embrace a new skill set, new vocabulary and a new perspective on where cybersecurity fits into the budget picture.

CFOs unquestionably care more deeply than ever about cash management (cash preservation, actually) and driving operating profit amid increasing market uncertainty. But the CFO has often been tasked with being on the cybersecurity team, especially as it relates to the essential risk management functions of compliance, legal and governance. And has there ever been a risk management challenge as meaningful as COVID?

We all have to find a way to work together to identify, protect against, and remediate the impact of cybersecurity risk. Many business leaders recognize that cybersecurity is more important than ever in an era of remote work. But with an uncertain economic landscape, it is critical to get alignment to the dramatic shift businesses have to make, earlier rather than later. Don't wait. Don't procrastinate. Don't delay having the occasional hard conversations. You may be surprised. At the end of the day, you want to build out your "Yes Team" to drive the organization toward safety and security, and having the proper investment and budget is absolutely essential. So go for it.

This article is excerpted from Matt's chapter in the book **Navigating the Digital Age, The Definitive Cybersecurity Guide for Directors and Officers, Third Edition**. *We invite you to download your free digital copy.*[2]

1. Richard Seiersen, "How to Optimize Cybersecurity Using Measurement," SecurityRoundtable.org, accessed January 9, 2023.
2. https://start.paloaltonetworks.com/navigating-the-digital-age-fy22.html

Matt Gyde is chairman and chief executive officer at Foresite MSP

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).

What Can Service Providers Do About 5G Security?

By Sean Duca

We're about to undergo one of the biggest generational changes in technology—the shift to 5G networks for mobile internet connectivity. It won't happen overnight, but it will happen over the next few years.

Now is the critical time for us to begin asking vital questions about security. Specifically, what role should service providers take to make these networks—and our world—as safe as possible.

5G networks offer the promise of dramatically faster and more reliable connections from mobile devices. Not just computers, laptops, tablets and smartphones, but the billions upon billions of connected devices that are already spreading like wildfire.

In a 5G network, every device has the potential for a speed of 100 megabytes per second. This will create an explosion of innovation and will make for ubiquitous connectivity for everything—human to human, human to machine, machine to machine. Autonomous vehicles will actually be able to work. Remote surgeries will be a real thing.

Don't just take my word for it. Here's what 451 Research has to say about 5G: "It will radically change the technologies and business models of the mobile telecommunications industry. More than that, 5G is widely expected to be a defining stage in the global evolution of IT in general, affecting almost all parts of industry and society."

But what about security? With ubiquitous connectivity and virtually unlimited bandwidth, what can we do to maximize protections?

5G networks don't just create opportunities for businesses, governments and other institutions to be innovative; they provide adversaries with a new platform for innovation—not to mention an attack surface that will be growing by the billions.

In the brave new world of 5G it is time for the telecommunications providers that are building these networks to step up. It is also time for government regulators to make sure service providers step up. Not two or three years down the road when deployments will be growing, but now, when the networks are being constructed and protections can be built in.

What, you may ask, can the service providers do? In the past, we haven't asked them to take on the role of securing the information highways they provide. Why should we ask that of them now?

Here's why:

1. **Because they can**. The technology is available for providers to visibly inspect everything traversing through their networks so that they can block malicious traffic where and when it is necessary to do so. 5G networks are built on software, so security can be deployed in different ways versus earlier generations.
2. **Because they should**: 5G networks will quickly become a vital part of everything we do. How we live, how we work; education, entertainment, healthcare, voting, defense, you name it. We will be dependent on these systems, so let's remove the need for users to think about security every time they log on. They still will, but let's make it easier—and safer.
3. **Because leaders must insist on it**. If you're a CEO or a CIO you will likely be putting all your chips at the center of the table with 5G, building business models that rely on the speed, reliability and availability of these networks. You can—and should—demand a clean pipe to the internet, free of malicious codes and security challenges. You can't afford to have any of your applications, workloads or data compromised.

Would you want your family traveling on a highway that doesn't have basic security protections, like lights or warning signs? Or course not.

Expecting the builders of the information highways to do basic inspection and prevention is not too much to ask. It is something each of us, as business leaders, security professionals or just plain technology users, should demand. Now is the time to make our voices heard.

1. Greg Day, "Security Chiefs: Don't Ignore the 5G Future, It's Coming Fast," SecurityRoundtable.org, accessed January 9, 2023.
2. https://451research.com/5g-innovation-disruption-and-opportunity-ahead (link broken)

Sean Duca is vice president, regional chief security officer, Asia Pacific and Japan, for Palo Alto Networks

Reprinted from Security Roundtable by Palo Alto Networks (SecurityRoundtable.org).

Cyber Perspectives Magazine

A print magazine featuring critical research and content for cybersecurity executives from industry experts

Subscribe to receive each new issue every quarter for **FREE** at register.paloaltonetworks.com/cyberperspectivesmagazine

paloalto® NETWORKS

THREAT-INFORMED
INCIDENT RESPONSE

Respond with confidence.
Partner with experts.

Learn more at paloaltonetworks.com/unit42

paloalto® NETWORKS | UNIT 42™ BY PALO ALTO NETWORKS