Cybersecurity in Public Sector: 5 Insights You Need to Know

SPONSORED BY TENABLE

Independently conducted by Ponemon Institute LLC

February 2019

Cybersecurity in Public Sector: 5 Insights You Need to Know

EXECUTIVE SUMMARY

Cybersecurity in Public Sector: 5 Insights You Need to Know,[1] sponsored by Tenable® and conducted by Ponemon Institute, reveals that public sector organizations are at serious risk for a cyberattack. They often lack the fundamentals to quickly respond to vulnerabilities and effectively mitigate their cyber risk. First and foremost, they frequently don't have sufficient visibility into their attack surface. They're also facing an understaffed IT security function and are dependent on manual processes.

After analyzing the survey responses from 244 public sector employees in the United States, United Kingdom, Germany, Australia, Mexico and Japan responsible for evaluating and/or managing their organizations' investments in cybersecurity solutions, we arrived at these five findings:

1. **Cyberattacks in the public sector are relentless.** Most public sector organizations have experienced a cyberattack. In fact, 88% of surveyed organizations have suffered at least one damaging cyberattack over the past two years. 62% have experienced two or more. These attacks have caused data breaches. They've also resulted in significant disruption and downtime to business operations as well as plant and operational equipment.

2. **Preventing attacks against IoT and operational technology (OT) infrastructure is a top priority for 2019.** When ranking their top cybersecurity concerns for 2019, nearly two-thirds (65%) of public sector respondents say they're worried about attacks involving IoT or OT assets. 61% are specifically concerned about attacks against OT infrastructure.

3. **Public sector cybersecurity teams face fundamental challenges managing cyber risk:**
    - Only 23% of respondents say they have sufficient visibility into their attack surface.
    - They lack adequate staffing and efficient processes to manage the endless backlog of vulnerabilities. 62% of respondents say their organizations' security function doesn't have adequate staff to scan for vulnerabilities in a timely manner.

4. **To help mitigate cyberattacks, new approaches for measuring cyber risks are needed.** Traditional KPIs or metrics for evaluating business risks cannot be used to understand cyber risks. Only one-quarter (27%) of respondents say their organizations can correlate information from cyber risk KPIs to mitigative actions on a data breach or security exploit.

5. **Smarter prioritization of vulnerabilities is key to staying ahead of cyberattackers.** 63% of respondents say they want to improve their ability to keep up with the sophistication and stealth of attackers. Yet, nearly half (44%) say they prioritize threats based on the ease of remediation – which is far from ideal. Rather, prioritization should be based on the threats that pose the greatest risk.

1 We surveyed 2,410 IT and IT security practitioners in the United States, United Kingdom, Germany, Australia, Mexico and Japan and the findings were presented in a previously released report, ***Measuring & Managing the Cyber Risks to Business Operations***. This report features the findings of 244 respondents in the public sector.

KEY INSIGHTS

Let's take a closer look at each of the findings.

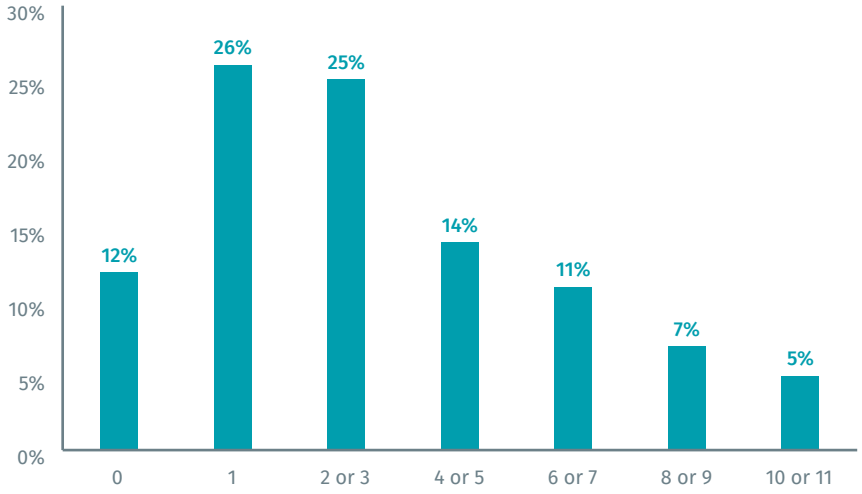
Finding #1: Cyberattacks in the public sector are relentless.

As shown in Figure 1, 88% of public sector organizations represented in this study have experienced at least one damaging cyberattack in the past two years, and 62% have had two or more. These attacks have resulted in data breaches and/or significant disruption and downtime to business operations, plants and operational equipment.

Figure 1.
Public sector organizations have experienced multiple damaging cyberattacks

Number of cyberattacks experienced over the past 24 months

88%
experienced at least one damaging cyberattack



Finding #2: Preventing attacks against IoT and OT infrastructure is a top priority for 2019.

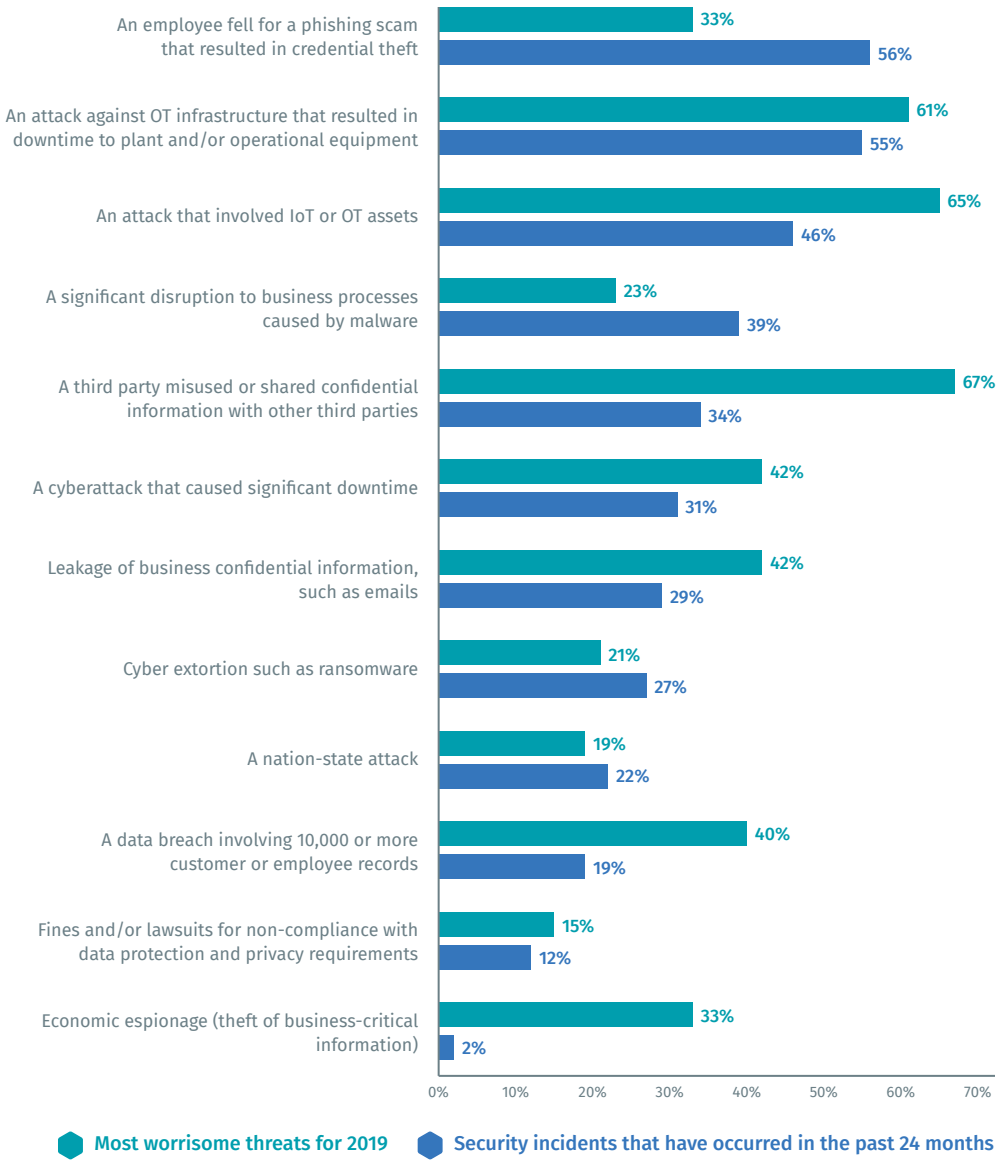
We asked respondents if their organization had experienced any of 12 different security incidents (see Figure 2) and to comment on which security incidents they're most concerned about in 2019. The top bar (in teal) represents the most worrisome threats for 2019, while the bottom bar (in blue) indicates the types of cyberattacks experienced.

As shown below, 65% of respondents worry about attacks involving IoT or OT assets. 61% are specifically concerned about attacks against OT infrastructure. Given that more than half (55%) of the public sector organizations surveyed had experienced an attack against OT infrastructure that resulted in downtime to plant and/or operational equipment, it's no surprise that protecting OT is top of mind.

Figure 2.
Most worrisome threats for 2019 and the security incidents public sector organizations have experienced

12 security incidents

65%
worry about attacks involving IoT or OT assets



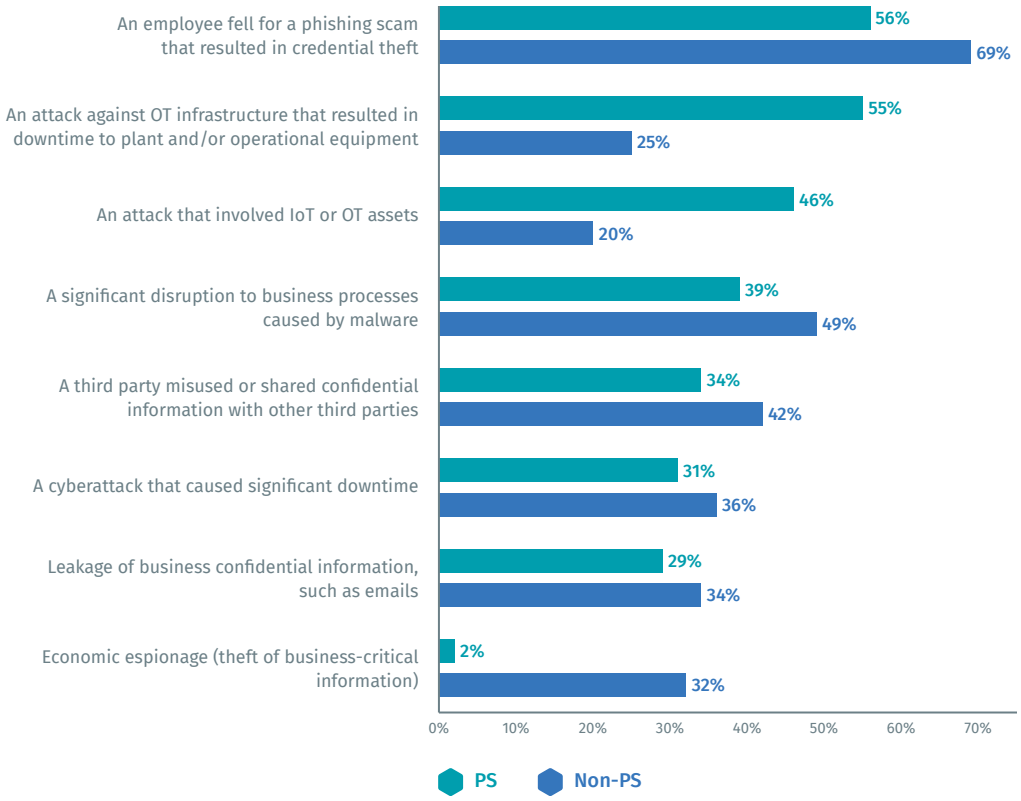
Public sector is more susceptible to cyberattacks against OT infrastructure and IoT/OT assets

As shown in Figure 3, cyberattacks are more likely to target the OT infrastructure and the IoT and OT assets in the public sector (vs the private sector). In fact, when it comes to attacks on OT that caused downtime, the survey shows the odds are almost double that of other sectors (55% vs 25%). Similarly, nearly half (46%) of public sector organizations experienced an attack involving IoT or OT compared to just one-fifth of the private sector.

Figure 3.
Has your organization experienced any of the following incidents in the past 24 months? (public sector vs private sector)

More than one response permitted

46%
experienced attacks involving IoT or OT

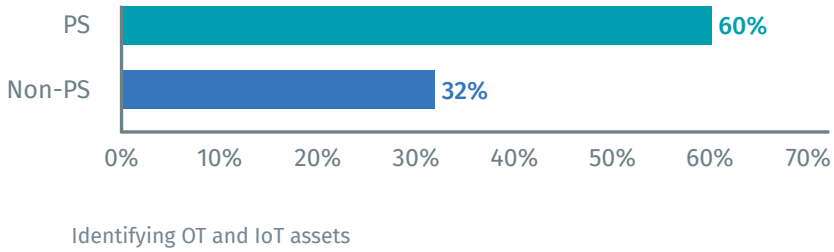


More public sector organizations use the identification of OT and IoT assets as a measure of success

In response to the barrage of OT attacks, public sector organizations are almost twice as likely to use the identification of OT and IoT assets as a KPI in assessing their cybersecurity posture (60% of public sector respondents vs 32% of respondents in other sectors). See Figure 4 below.

Figure 4. KPIs used by organizations (public sector vs private sector)

Public sector 2x as likely to use identification of OT/IoT assets as measure of success



Identifying OT and IoT assets

Finding #3: Public sector cybersecurity teams face fundamental challenges managing cyber risk.

To gain a deeper understanding of what it's like to be on the front lines of cyber defense, we asked respondents to share their perceptions about responding to vulnerabilities and threats. Here's what they have to say.

Insufficient visibility into the attack surface

Only 23% say they have sufficient visibility into their attack surface (see Figure 5), which means the majority of public sector organizations do not have a holistic view of their cyber risk – across cloud, containers, IoT and OT. Without this essential foundation in place, security teams do not have a complete picture of the risk landscape.

Only 23% have sufficient visibility into their attack surface

Manual processes are causing an insurmountable backlog of work

In addition to the visibility issue, public sector security teams face a vulnerability overload problem, as indicated in Figure 5 below. 56% of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes. And 51% of respondents say security spends more time navigating manual processes than responding to vulnerabilities – resulting in an insurmountable backlog.

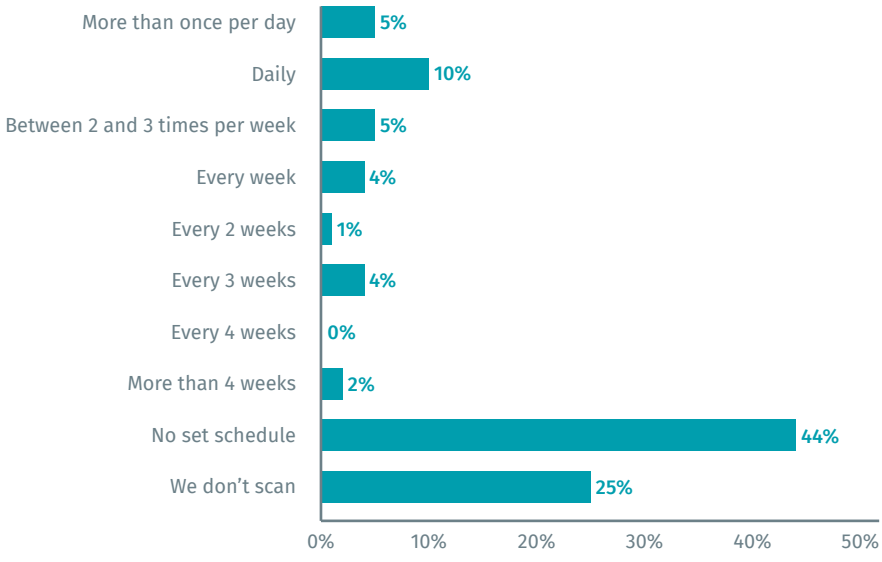
Figure 5. Perceptions about responding to vulnerabilities and threats

Understaffing means under scanning

Moreover, shortages in staffing hinder the public sector's ability to quickly scan for vulnerabilities. 62% of respondents say their organizations' security function doesn't have adequate staff to scan for vulnerabilities in a timely manner. 69% of respondents say their organizations have no set schedule to scan (44%) or do not scan at all (25%). See Figure 6.

Figure 6.
How quickly does your organization scan for vulnerabilities once they have been publicly disclosed?

69%
of respondents have no set schedule or don't scan
(44% + 25%)



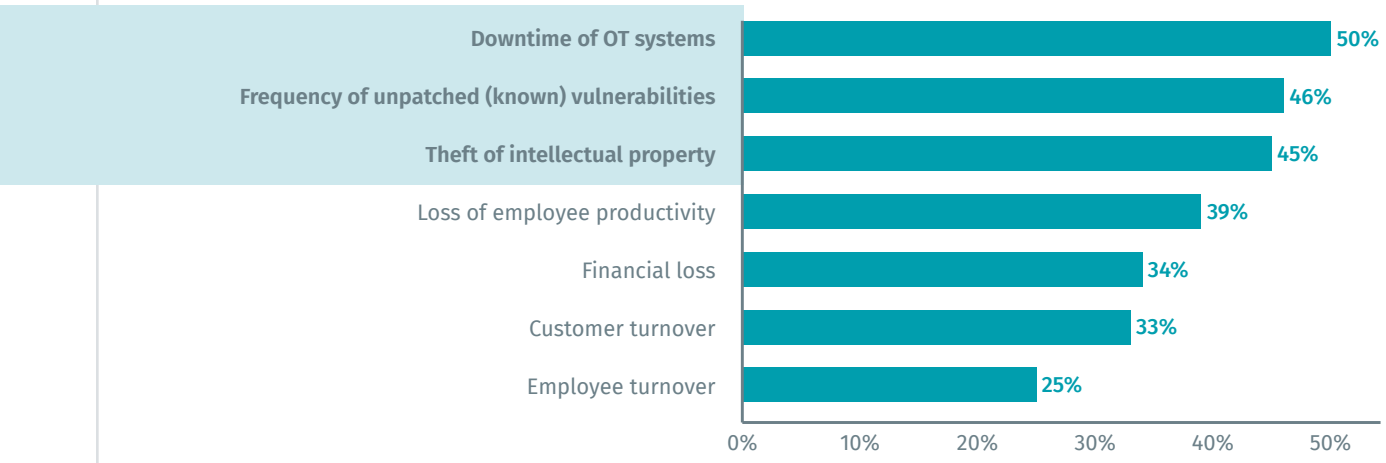
Finding #4: To help mitigate cyberattacks, new approaches for measuring cyber risks are needed.

Most organizations aren't quantifying what a security incident would cost

Only 40% of respondents say their organizations attempt to quantify the damage the 12 incidents listed previously (see Figure 2) could have on their businesses. The factors these organizations use to quantify the risk are listed in Figure 7. Of the respondents who say their organizations attempt to quantify security incidents, they focus on these primary factors:

- 50% quantify what the downtime of OT systems would cost
- 46% calculate the frequency of unpatched (known) vulnerabilities
- 45% quantify the theft of intellectual property

Figure 7. What factors are used to quantify the potential risk of a cyberattack?



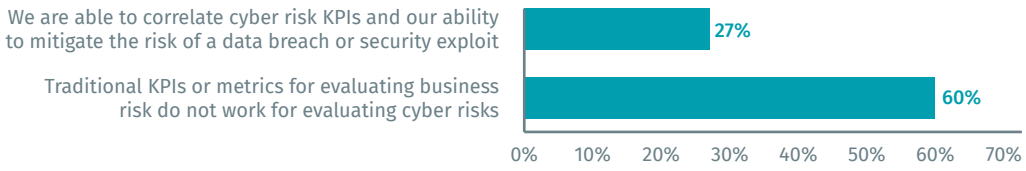
More than one response permitted

To help mitigate cyberattacks, new approaches for measuring cyber risks are needed

As shown in Figure 8, traditional KPIs or metrics for evaluating business risks cannot be used to understand cyber risks. Only one-quarter (27%) of respondents say their organizations can correlate information from cyber risk KPIs to mitigative actions on a data breach or security exploit.

Only 27% say they can correlate information from cyber risk KPIs to mitigative actions on a data breach or security exploit

Figure 8. Perceptions about KPIs



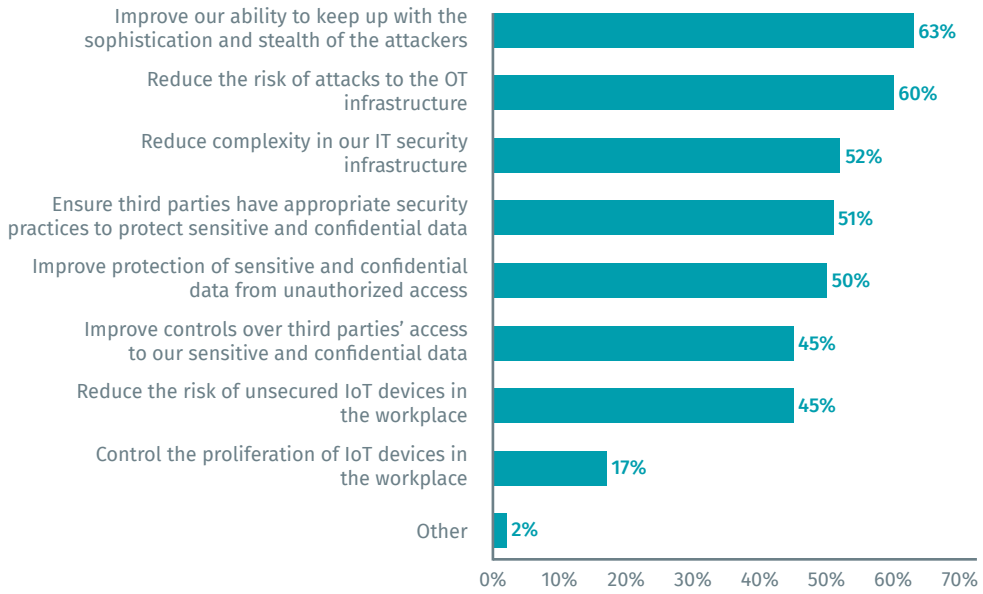
Strongly Agree and Agree responses combined

Finding #5: Prioritization of vulnerabilities is key to staying ahead of cyberattackers.

As shown in Figure 9, 63% of respondents say they want to improve their ability to keep up with the sophistication and stealth of attackers.

Figure 9.
The top eight security priorities for 2019

More than one response permitted



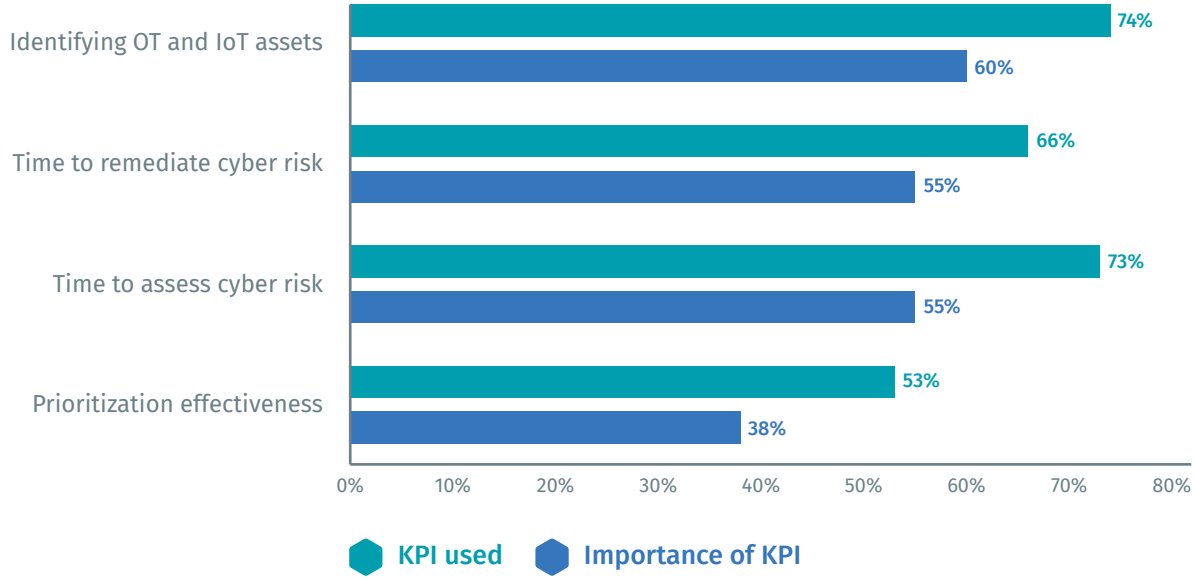
63%
want to improve their ability to keep up with the sophistication and stealth of attackers

There's a gap between the KPIs the public sector wants to use versus what they're actually using

Unfortunately, public sector organizations aren't using the KPIs they consider most important to assessing and understanding cyber threats. We asked respondents if their organizations are using the KPIs listed in Figure 10 and to rank how essential these KPIs are to minimizing cyber risk on a scale of 1 = not important to 10 = essential.

As shown below, there's a significant gap between the use of these KPIs and their perceived importance, especially with respect to measuring the time to assess cyber risk, identifying OT and IoT assets and prioritization effectiveness.

Figure 10. Gap in the use and importance of KPIs



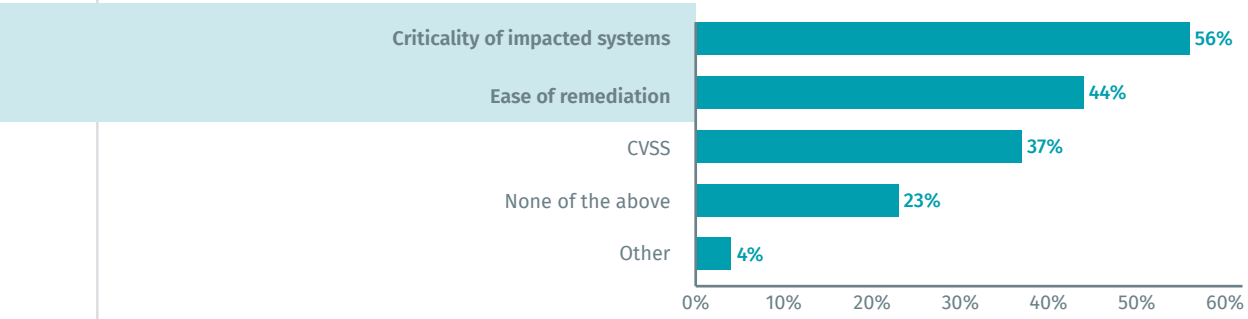
Yes responses and Very Important and Essential responses presented

There's also a disconnect in how organizations say they're prioritizing threats

Respondents could select more than one choice to indicate how their organizations prioritize threats to critical business assets. 56% of respondents say their organizations consider the criticality of affected systems – which we consider to be an indicator of a mature cybersecurity posture. See Figure 11.

Meanwhile, 44% of respondents say they prioritize based on the ease of remediation – which we consider to be the least-mature approach to prioritization and potentially leaves the organization vulnerable to actual risks.

Figure 11. How does your organization prioritize threats to critical business assets?

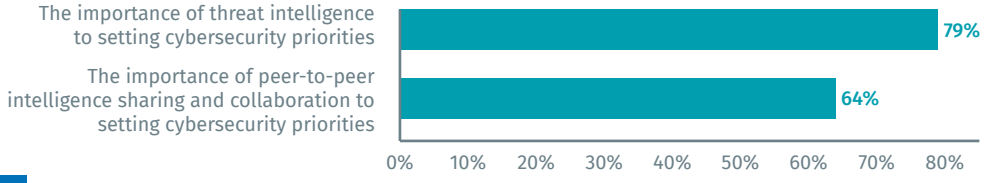


More than one response permitted

Threat intelligence is essential

Respondents were asked to rate the importance of threat and peer-to-peer intelligence sharing on a scale of 1 = not important at all to 10 = essential. As shown in Figure 12, 79% of respondents say threat intelligence is very important or even essential. Meanwhile, 64% say peer-to-peer intelligence sharing and collaboration is important for setting cybersecurity priorities.

Figure 12. Importance of threat and peer-to-peer intelligence sharing



From 1 = Not important at all to 10 = Essential, 7+ responses presented

79%
say threat intelligence is very important or even essential

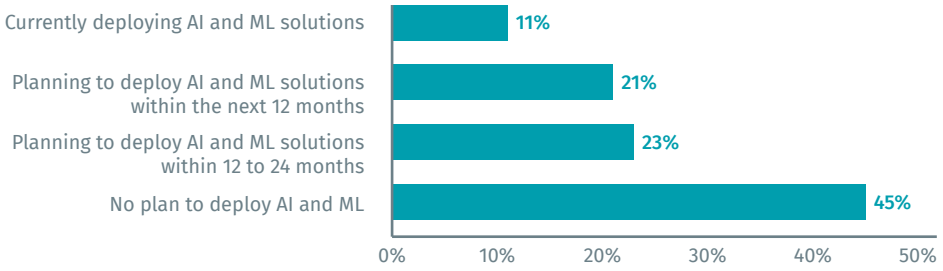
Organizations are looking toward AI and machine learning for smarter vulnerability management and prioritization

55% of respondents say they're currently deploying AI and machine learning (ML) solutions – or plan to within the next two years. See Figure 13.

55%

say they're currently deploying or planning to deploy AI and machine learning solutions
(11% + 21% + 23%)

Figure 13. Does your organization plan to use AI and ML for vulnerability management?



CONCLUSION

This study reinforces the belief that public sector technology leaders face near-continuous cyber threats and attacks. It also acknowledges that these leaders now consider threats against OT more concerning than threats against traditional IT. This is a result of a couple of key factors:

- First, the swift pace of digital transformation in the public sector has created a corresponding expansion of the cyberattack surface – with more IoT and OT devices being used to improve constituent services.
- Second, public sector IT leaders are increasingly being asked to manage a converged IT/OT environment, requiring them to adopt methods and approaches that meet threats effectively while maximizing service availability to constituents.

Here are two promising approaches for enabling management of vulnerabilities holistically across the attack surface:

- **Predictive Prioritization:** The number of vulnerabilities has nearly doubled in the past two years. But, the number of vulnerabilities being exploited is only a small fraction of the total. Predictive Prioritization help you zero in on remediating the vulnerabilities that matter most. **Learn more.**
- **Passive monitoring:** Typically, security leaders can't actively scan OT environments due to potential service interruptions. Fortunately, passive monitoring can provide much-needed visibility into OT environments. **Learn more.**

These two approaches, married with advanced analytical and reporting tools, will serve public sector security leaders well as they build the information security programs of the future.

Please write to **research@ponemon.org** or call **800.887.3118** if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advance responsible information and privacy-management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

Ponemon INSTITUTE

COPYRIGHT 2019 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.