SOLUTION BRIEF

Make FortiGuard Incident Readiness Assessments an Integral Part of Your Security Strategy

Executive Summary

It's what you don't know that can hurt you the most

Whether enterprises are dealing with digital transformation or adapting to a pandemic, change remains a constant. To meet the needs of today's rapidly evolving digital marketplace, organizations need to be able to pivot quickly while keeping their cybersecurity posture resilient. That's because the cost and impact of cyber incidents, from web application attacks to data breaches, continue unabated. There is a lot at stake, so enterprises must stay vigilant to their changing security posture while constantly working to discover and immediately address any gaps or weaknesses, identifying and responding to cyber events before they impact the company.

Against the backdrop of today's continuous change, readiness assessments play a vital role in educating security leaders about quantifiable system vulnerabilities and providing prioritized actions for closing those gaps. **FortiGuard Incident Readiness Assessments** play an integral role in your security hygiene best practices, especially as the network, people, processes, and threats evolve. But to be helpful, these assessments must guide and prescribe rather than overwhelm, helping security leaders make informed, prioritized decisions to protect their business.

According to ISACA, "Conducting cyber-risk assessments is critical to effective monitoring of risk factors and to improving response capabilities."[1]

Are You Prepared for the Inevitable Cyberattack?

The prevalence and potential impact of a cyberattack should be an ongoing enterprise concern, regardless of the type of incident. Today's enterprises are dynamic, living entities, combining rapid business evolution and expanding hybrid networks with a work-from-anywhere workforce, shortfalls in security staff resources and skillsets, and employee turnover. From cloud adoption and application migration to digital transformation initiatives to mergers and acquisitions, constant change makes it difficult for security leaders to maintain a static and consistent state of security. It's why nearly half of executives surveyed feel that their security has not "kept up with digital transformation."[2]

So what can security leaders do to ensure that their enterprise risk levels remain low and their business remains viable regardless of their ongoing digital metamorphosis?

It starts with understanding the scope and scale of the challenges being faced. An Incident Readiness Assessment is a valuable tool for helping you know what risks your organization faces and determining your ability to withstand and respond to an attack. As Plato said, "Ignorance is the root of misfortune." By providing a clear and current view of how your cybersecurity posture has evolved as your enterprise is transformed, security leaders can better understand the gaps they must address and prioritize addressing the most-critical issues first. To achieve this, however, an effective assessment must include prioritized, quantifiable improvements designed to return the organization to an acceptable risk level, as defined by the business.

Making Time for This Critical Step

While the lack of personnel and essential security skills are often cited as reasons for not conducting regular assessments, outsourcing this process to security experts can effectively address these concerns. And when a professional team is engaged, a third concern—downtime—is also addressed as the *actual* time needed ends up being far less than anticipated.

However, it is vital to recognize that an effective assessment is not a "once and done" proposition. Depending on the rate of change affecting today's organization, assessments should be conducted more than once a year. According to ISACA, an "[annual] interval is not optimal. It allows too much time for significant environmental deviations to occur, which could weaken response plans and undermine organizational resilience".[3] Instead, the cadence of assessments should be determined by your enterprise culture, the level of change in a given year, and other factors (adopting new technologies, a merger or acquisition, etc.). Many organizations now include bi-annual assessments in their cyber-posture-update planning.

And as for downtime, while an outside assessment team will require time to lead discussions, analyze inputs, and prepare findings, the commitment from the enterprise team can be as little as a week for initial stakeholder discussions and an hour for the report read-out. And those discussions can be spread out or compressed into as little as a week, depending on your schedule. And subsequent assessments build on that initial discovery, which means the entire process becomes more efficient over time.

But more importantly, it is helpful to compare your investment in a professional assessment to the potential downtime (and cost) associated with an inadequate response to a cyber incident. This exercise will demonstrate a significant return on investment, especially when considering the opportunity to address gaps or weaknesses *before* they become a consequential liability that can interrupt business, impact brand, and result in other costly effects.

Further, proactively selecting who will conduct these assessments is another critical element of this process. You know your organization better than anyone. Most organizations prefer choosing who and when they hire an assessment team for such an important task—rather than having those resources selected for you by someone outside your company, such as an insurer or incident response agency.

The Assessment Process

In today's world, a security breach is not a matter of "if but when," even with the best security technologies. The trick is to minimize its impact. This includes having a plan for managing a cyber incident, such as establishing the chain of command, outlining communications protocols, and protecting, collecting, and analyzing forensic evidence. Our Incident Readiness Assessment focuses on improving the implementation and management of these and other incident response strategies.

FortiGuard assessors use accepted standards, including those from the National Institute of Standards and Technology (NIST), as the foundation of their process. But our FortiGuard team is also actively helping organizations recover from cyber incidents. Combining the expertise and best practices that can only be developed through conducting thousands of incident investigations with a deep understanding of incident response processes can significantly limit the impact of an incident, shorten downtime during an investigation, and accelerate recovery.

The FortiGuard assessment framework comprises six functional domains used to assess the state of the organization. These best practices have been derived from official guidance combined with the experience of seasoned FortiGuard incident response experts who help clients deal with cyber incidents every week. These responders have developed in-depth knowledge of how malicious actors enter an environment, maintain their presence, move laterally, and escalate privilege. This expertise helps them fine-tune your incident response strategy and identify gaps that most enterprises (and other assessment teams) miss.

Incident Readiness Assessment Domains	
Event and Incident Response	Threat and Vulnerability Management
Asset Management	Continuity of Operations and Disaster Recovery
Identity and Access Management	Network Security

Their incident response assessment process gauges your organization's overall ability to prevent as well as respond efficiently and effectively to an unexpected cyber incident—all in less than a week. Or they can work around your schedule to keep the impact on your business to a minimum. The assessment process includes a document review combined with focused stakeholder interviews for clarifications and to answer final questions. Assessors then establish a baseline, such as the existence of playbooks and incident response planning, help identify gaps and their potential impact, and then prioritize actions to help mitigate the risk based on the results.

The incident readiness final report provides maturity scoring using a proprietary tool that allows easy visualization at a high level and helps set prioritized, actionable recommendations designed to return the most value for effort and resources. This report also identifies specific areas of your incident response processes and procedures to strengthen, helping you to improve your overall cybersecurity program, prioritize cybersecurity actions and investments, and maintain the desired level of business continuity and recoverability during an unexpected cyber incident.

"A risk assessment can quickly identify and prioritize cyber vulnerabilities so that you can immediately… protect critical assets… while immediately improving overall operational cybersecurity."[4]

Assessment Outcomes and Service Options

Indeed, today's enterprise is in constant flux—as is the threat landscape. Incident Readiness Assessments provide a snapshot of your current risk amid this sea of change. They provide prescribed actions designed to help security leaders make prioritized, impactful decisions that can mean the difference in the continuity of their business operations.

For a more comprehensive approach to incident preparedness, FortiGuard offers the choice of standalone assessments or the option of a subscription service. The FortiGuard Incident Readiness Subscription Service enables security leaders to prepare better, respond rapidly, and take effective actions at every step. The one-year subscription provides a comprehensive set of services that can include some of the following:

- One readiness assessment
- Incident response playbook development
- Incident response playbook testing (tabletop exercises)
- Digital forensics and incident response (with a one-hour service-level objective)

  *Additional hours may be purchased as needed.

Conclusion

Given today's statistics of cyberattack costs and prevalence, Incident Readiness Assessments are essential, providing enterprises with a clear view of their gaps and actionable recommendations to ride out the next attack wave. Organizations can no longer afford to operate from a position of ignorance is bliss. Instead, calculated planning based on accurate data and years of expertise must be the theme of any cybersecurity plan. This is the only approach that can lead to peace of mind.

[1] ISACA State of Cybersecurity 2022.

[2] ThoughtLab 2022 Report, "Cybersecurity Solutions for a Riskier World."

[3] ISACA State of Cybersecurity 2022.

[4] Chuck Brooks, "A Cybersecurity Risk Management Strategy for the C-Suite," Homeland Security Today, May 11, 2022.

December 8, 2022 1:49 PM

1852116-0-0-EN