Assessing your cybersecurity posture: The processes and frameworks you need

BY ANNA HAMMOND · AUGUST 15, 2024 · LAST UPDATED ON MAY 13, 2025

There's a lot being written about the need for strong cyber resilience, and with good reason. Cyber resilience offers several key benefits for organizations, strengthening their ability to handle cyber threats effectively while reducing the risk of business disruption. With the average data breach cost reaching $4.45million in 2023, according to IBM, there's more than enough motivation for businesses to take it seriously.

To enhance your organization's cybersecurity and resilience, it's crucial to first understand its current security stance. To get this insight, you'll want to run a security posture assessment. This guide will take you through the process step-by-step, helping you grasp the essential elements of what a good assessment looks like.

A short introduction to cybersecurity posture

Think of an organization's security posture as the immune system of a living organism. Just as the immune system works to protect the body from illness and recover quickly when sickness strikes, a strong security posture safeguards an organization's software, networks, services, and information. It includes a robust set of policies, controls, and technologies designed to ward off threats and efficiently manage any breaches that occur.

But it doesn't stop there; like a vigilant doctor who keeps up with the latest medical research, a strong security posture requires ongoing assessment and enhancement to adapt to new threats and vulnerabilities. This proactive approach ensures that an organization can effectively defend itself against cyber-attacks and minimize their impact if they do occur.

What is a security posture assessment?

A security posture assessment is a comprehensive evaluation of an organization's cybersecurity strengths and vulnerabilities. It involves reviewing and analyzing the security measures currently in place to protect against threats and vulnerabilities. The assessment covers various aspects, including technical defenses, security policies, user access controls, and response strategies.

The goal is to identify any weaknesses or gaps in the security framework that could be exploited by attackers and to recommend improvements to enhance the organization's overall security posture. This process helps to ensure that the organization can effectively protect its assets and maintain resilience against cyber threats—much like maintaining strong locks, surveillances, and alarms to keep a home safe from intruders.

When to assess cybersecurity posture

Given the dynamic nature of cyber threats, regular assessments should be a routine part of your security strategy. The frequency—whether annual, semi-annual, or quarterly—depends on the organization's size and complexity. However, there are some key times when a security posture assessment is particularly crucial:

- After a security incident
- For compliance
- Following major organizational changes
- During business expansion
- Cybersecurity leadership changes
- Before integrating new systems.

Cybersecurity posture assessments in these scenarios allow security teams to maintain robust defenses, adapt to new challenges, and ensure continuous protection against cyber threats.

Security posture assessment checklist

Intigriti's security posture checklist will steer you through the essential aspects to consider during the process, ensuring a thorough evaluation of your cybersecurity landscape. Plus, we've illustrated how items on the checklist can be applied with concrete examples.

Step 1: Goal setting and business context gathering

Before diving into the technical details, it's crucial to understand the business context of your organization. This involves identifying the core business objectives, understanding the industry-specific risks, and recognizing the assets that are most critical to your business operations. Here's some examples of how a business might apply this step:

- **Align goals with business objectives:** A financial services firm might set a goal to achieve zero data breaches in the year, directly supporting its objective of maintaining customer trust.
- **Industry-specific risks:** A healthcare provider needs to consider risks related to protected health information (PHI), which is highly targeted by cybercriminals.
- **Critical business assets and operations:** This could include identifying key data centers and proprietary software for a tech company.

It's important not to miss this step. Setting clear goals for the assessment will align the security measures with the business needs, ensuring that the cybersecurity strategy supports overall business objectives.

Step 2: Identify and categorize assets

Next, create a detailed inventory of all assets within the organization, including hardware, software, data, and network resources. Categorizing these assets based on their criticality and sensitivity helps in

prioritizing security efforts. Here's how that might look like in practice:

- **List all hardware assets and categorize by importance:** A retail company might list servers that process payment transactions as high importance.
- **List all software assets, including applications and operating systems:** This might include documenting all instances of customer relationship management (CRM) software in use.
- **Identify and classify data based on sensitivity and regulatory requirements:** For example, classifying customer financial information as high sensitivity and ensuring it is handled per GDPR or CCPA.

This task might take a bit of time, but once you're done, keeping up and boosting your cybersecurity becomes a whole lot easier. You'll have set the stage for smoother and more effective security management down the line.

Step 3: Conduct vulnerability assessments

The next step is vulnerability mapping. This task focuses on pinpointing threats and weaknesses that might undermine your organization's cybersecurity defenses.

Threats could come from cybercriminals, natural disasters or system malfunctions, for example, whereas vulnerabilities might stem from improper configurations, obsolete software, or frail passwords. Recognizing these threats and vulnerabilities is essential for devising specific countermeasures and mitigation strategies.

Carry out threat modeling exercises and conduct vulnerability assessments. Challenges you might encounter include new or evolving threats, insufficient insight into your infrastructure, or subpar vulnerability scanning tools. To counteract this, you could also execute penetration tests and bug bounty programs to uncover potential risks.

Here are some practical examples to illustrate this:

- **Threat modeling:** A financial institution might use threat modeling to simulate attacks on its online banking system. This could involve mapping out potential entry points for hackers, such as through phishing attacks targeting bank employees or through vulnerabilities in the mobile banking app.
- **Penetration tests:** An eCommerce company might hire external security experts to perform penetration testing on its website. These experts would attempt to breach the website's security controls using the same techniques a hacker might use, helping to identify weak points in the site's defenses.
- **Bug bounty programs:** A streaming-service might launch a bug bounty program, inviting ethical hackers from around the world to find and report security flaws in return for rewards based on the severity of the vulnerabilities they discover.

Essential resources for this task could include access to threat intelligence services, systems for managing vulnerabilities, tools for conducting penetration tests and bug bounty programs, or crowdsourced security service providers.

Step 4: Review existing security policies and procedures

Evaluate the current security policies, procedures, and controls to determine their effectiveness in addressing identified risks. Here are some examples of what should be analyzed during this stage:

- **Review and document existing security policies and procedures:** Checking if the current incident response plan includes steps for containment and eradication.
- **Assess the effectiveness of current security controls:** Evaluating whether existing firewalls and intrusion detection systems are effectively blocking threats.
- **Identify any gaps in current security practices:** Noticing that 2FA (two-factor authentication) is not used for accessing internal databases and planning to implement it.

Understanding these processes helps in identifying gaps in your security posture and provides a baseline for improvement.

Step 5: Assess network architecture and controls

Examine the security of your network architecture, including firewalls, routers, and switches. Ensure that proper segmentation is in place to protect sensitive data and systems from unauthorized access. Network security assessments should also include the evaluation of wireless networks and remote access protocols.

Step 6: Implement data security measures

Assess the measures in place to protect data at rest, in transit, and during processing. Encryption, access controls, and data masking are some of the techniques that should be evaluated to ensure that data is adequately protected against breaches and leaks.

Step 7: Training and awareness in the organization

Human error is a significant factor in many security incidents. Conducting regular training and awareness programs for all employees helps in building a security-conscious culture within the organization. These programs should cover topics such as password management, safe internet practices, and phishing simulations.

For example, a media company might conduct monthly phishing simulations for all employees to help them recognize suspicious emails. This could involve sending fake phishing emails that mimic common tactics used by cybercriminals. Employees who click on links in these emails are then provided with immediate training on how to identify and avoid real phishing attempts in the future.

An IT firm could host quarterly workshops focusing on strong password creation and the importance of using different passwords for different accounts. These workshops might also introduce employees to tools like password managers that can help in generating and storing complex passwords securely.

An organization that is mostly remote might include sessions on safe internet practices. These sessions could cover topics such as secure browsing, the risks of downloading unauthorized software, and the importance of regularly updating device security settings.

Each of these examples shows how targeted training and awareness programs can address specific aspects of cybersecurity, thereby fostering a more security-conscious culture within the organization.

Step 8: Ensure compliance with legal and regulatory standards

Depending on your industry and location, there may be various legal and regulatory requirements related to cybersecurity. Assess your compliance with standards such as GDPR, HIPAA, or PCI-DSS, and identify necessary steps to meet these requirements.

Step 9: Evaluate third-party risks

Vendors and other third parties can pose significant security risks. Assess the security measures of your vendors and ensure they meet your security standards. You should be implementing strong contracts and continuous monitoring to manage these risks effectively.

Steps to take during this stage are:

- **Assess the security posture of key vendors and third parties:** Conducting security audits of vendors who handle sensitive data.
- **Identify steps to strengthen security clauses in vendor contracts:** Including requirements for vendors to adhere to specific security standards and to report security incidents. For example, by drafting a cybersecurity Service-Level Agreement.
- **Explore processes for ongoing vendor risk management:** Establishing regular reviews and updates of vendor security practices.

Step 10: Choose appropriate security frameworks

Selecting the right frameworks is crucial for a structured and effective assessment. For example, a government contractor might select NIST SP 800-171 to comply with federal requirements. However, you should choose a framework that aligns with your business needs and regulatory requirements.

Cybersecurity maturity models and frameworks

While each of these frameworks and models has its specific focus and requirements, they all aim to provide organizations with the tools needed to assess, manage, and improve their cybersecurity posture. By adopting one or more of these frameworks, organizations can better protect themselves against cyber threats, ensure compliance with regulatory requirements, and build trust with customers and partners.

NIST Cybersecurity Framework (CSF)

Developed by the National Institute of Standards and Technology, the NIST Cybersecurity Framework is highly regarded for its comprehensive and flexible approach to cybersecurity. Primarily aimed at improving the cybersecurity of critical infrastructure in the United States, it has been widely adopted across various sectors due to its applicability to different types of organizations.

The NIST CSF is organized into five core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

These functions provide a high-level strategic view of the lifecycle of an organization's management of cybersecurity risk. The framework helps organizations assess their current capabilities and maturity in each area, set goals, and prioritize improvements based on their specific needs and risk environment.

ISO 27001

ISO 27001 is an international standard for managing information security. It provides a set of standardized requirements for an Information Security Management System (ISMS). The standard is designed to help organizations secure their information assets such as financial information, intellectual property, employee details, or information entrusted by third parties.

Unlike the NIST CSF, which is more flexible, ISO 27001 requires compliance with a specific set of criteria, including a comprehensive assessment of information security risks and the implementation of detailed controls to mitigate these risks. Certification against ISO 27001 is recognized worldwide as an indication of a robust information security posture.

COBIT 5

COBIT (Control Objectives for Information and Related Technologies) is a framework for IT management and governance created by ISACA. COBIT 5 provides principles, practices, analytical tools, and models designed to help business leaders address the needs of all stakeholders across the enterprise IT. It extends beyond cybersecurity to encompass broader IT management issues, including risk optimization, resource management, and information governance.

The framework is particularly well-suited for organizations looking to align IT management with business objectives and ensure compliance with regulatory requirements.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. The standard is mandatory for all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers.

PCI DSS provides a baseline of technical and operational requirements designed to protect account data and includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

Compiling your findings and presenting the data

By now you should have your findings and have chosen a framework that works for you. The next step is to present them in a meaningful way to ensure it is both engaging and informative for all stakeholders, including those without a technical background.

Creating a comprehensive report from a security posture assessment involves clear structure, accessible language, and strategic presentation of data. Here's how cybersecurity professionals can effectively compile, structure, and present their findings:

1. Compilation of findings

Start by gathering all the data collected during the security posture assessment. This includes vulnerabilities detected, the impact of potential threats, and an evaluation of existing security measures. Organize this data into categories such as risk levels, affected systems, and recommended actions. Using your chosen cybersecurity framework can help in structuring this information systematically.

2. Report structure

The report should have a clear and logical structure, making it easy to follow. A typical layout might include:

- **Executive summary:** Provide a high-level overview of the assessment's key findings, risks, and recommendations. This section is crucial for senior management understanding and decision-making.
- **Methodology:** Briefly describe how the assessment was conducted, including the tools and techniques used. This adds credibility to your findings.
- **Detailed findings:** Present the data categorized by risk level or business unit. Use charts, graphs, and tables for better clarity.
- **Recommendations:** List actionable steps based on the findings. Prioritize these recommendations to help guide immediate actions and long-term planning.
- **Appendices:** Include detailed technical data or additional information here for those who might seek a deeper understanding or verification of the data.

3. Make it engaging and understandable

To ensure the report is accessible to non-technical stakeholders, avoid jargon and use plain language. Visual aids like infographics, charts, and graphs can help illustrate complex data points clearly. Including real-world examples or analogies can also make technical vulnerabilities more relatable.

4. Presentation and gaining buy-in

Presenting the findings internally involves not just sharing information but also persuading decision-makers of the urgency and importance of acting. Prepare a presentation that highlights the most critical

findings and their potential impact on the organization. Focus on how security improvements can lead to benefits like enhanced compliance, reduced risk, and protection of company reputation.

During the presentation, be prepared to answer questions and provide clarifications. Show how the recommendations align with business objectives and offer a clear return on investment. This alignment helps in gaining buy-in from various stakeholders across the organization.

How Intigriti can help

At the heartbeat of Intigriti's bug bounty platform is its 100,000+ ethical hacking community. We have successfully initiated more than 400 bug bounty and hybrid pentesting programs for leading brands like Microsoft, Ubisoft, Coca-Cola, and others. This proactive strategy not only bolsters security defenses but also ensures systems are up to date with the latest protections, significantly enhancing our customers' overall security posture.

To speak to a member of our team about leveling up your security testing methods, **get in touch** today!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com