UNIT V

SECURITY ASSESSMENT

Security Audit

Cyber security audits are a vital component of an organisation's defences against data breaches and privacy violations.By probing organisations' systems and services, an auditor can identify security weaknesses, and determine whether their practices comply with relevant laws, such as the GDPR (General Data Protection Regulation).

What is a cyber security audit?

A cyber security audit is a comprehensive review of an organisation's IT infrastructure. Audits ensure that appropriate policies and procedures have been implemented and are working effectively.

The goal is to identify any vulnerabilities that could result in a data breach. This includes weaknesses that enable malicious actors to gain unauthorised access to sensitive information, as well as poor internal practices that might result in employees accidentally or negligently breaching sensitive information.

As part of their review, the auditor will assess the organisation's compliance posture. Depending on the nature of the organisation, it could be subject to several information security and data privacy laws, creating a complex net of requirements.

The audit should be performed by a qualified third party. The results of their assessment act as a verification to management, vendors and other stakeholders that the organisation's defences are adequate.

Benefits of a cyber security audit

The main reason to conduct a cyber security audit is identify and address security and compliance weaknesses.

With a thorough assessment, the organisation will gain a comprehensive overview of their systems and gain insights on the best way to address vulnerabilities.

This mitigates the risk of a data breach and the repercussions that come with that. For example, a security incident can result in significant financial damage, which could have a lasting effect.

But it's not just the threat of business disruptions and regulatory fines that organisations need to be concerned about.

A security incident – particularly one that resulted from a preventable error – is likely to leave suppliers and customers less confident in the organisation. If the incident was serious enough, those stakeholders might even decide to take their business elsewhere.

The same applies for regulatory failures. If the organisation can demonstrate that it took appropriate steps to address data protection, regulators are unlikely to levy significant fines.

However, if the incident was the result of negligence, organisations could face stronger penalties. Even if those penalties don't approach the maximum allowable under the GDPR (€20 million or 4% of the organisation's annual global turnover), a comparatively lenient fine can still be disastrous.

With a cyber security audit, organisations can identify any non-compliant processes, whether that's in relation to the GDPR, the UK Data Protection Act or another law.

What does a cyber security audit cover?

A cyber security audit primarily covers an organisation's IT systems. This includes its infrastructure, the software it has deployed and the devices that employees use.

However, this is only one aspect of information security, and a comprehensive assessment won't stop at technical resilience. It will also assess:

- Data security: network access controls, data encryption and the way sensitive information moves through the organisation;
- Operational security: information security policies, procedures and controls;
- Network security: network controls, antivirus configurations and network monitoring;
- System security: patching, privileged account management and access controls; and
- Physical security: the organisation's premises, and physical devices that are used to store sensitive information.

Each aspect of the audit ensures that the relevant controls are in place, optimised and implemented in line with regulatory requirements.

How often should you conduct a cyber security audit?

Organisations should conduct a cyber security audit at least once a year. However, more frequent audits may be necessary depending on several factors.

One of those factors is the organisation's size and its available resources. Audits are extensive processes that can cost a lot of money, so smaller organisations are less able to perform regular audits.

By contrast, large organisations typically have the wherewithal – and the need – to conduct audits more frequently. With a greater number of systems and more complex procedures comes an increased cyber security risk.

Organisations should also conduct a cyber security audit whenever they make significant operational changes. An audit is also advisable if a new version of a compliance standard is released.

Cybersecurity Performance Management

Cybersecurity performance management is the process of evaluating and overseeing the effectiveness of your security program. It can be a challenge to manage, as the usual performance management indicators — cost and revenue — don't apply. Additionally, the field is always

changing; new technologies evolve and threats are advancing quickly. It's easy to be taken by surprise, and in light of this constantly-changing threat landscape, it may be hard to know how your cybersecurity program is performing. Cybersecurity performance management is possible, however.

If you're going to manage your cybersecurity program's performance you have to be able to measure it. Fortunately, there are metrics that will help you manage your cybersecurity performance. You just have to choose the ones that are relevant to your organization.

Why is cybersecurity performance management important?

Good cybersecurity performance management tells you where your security program is succeeding, where your weak spots are, and helps your security team and leadership understand what steps you need to take to make your cybersecurity program stronger.

This is done by measuring your information security program against key performance indicators (KPIs), such as:

- The time it takes to detect security-related incidents
- The time it takes to respond to security incidents
- Number of reported incidents
- The number and frequency of unreported incidents discovered after the fact
- Awareness of possible threats
- Level of preparedness
- Security training results
- The absence of unexpected security incidents
- Your organization's security rating

These aren't necessarily the only metrics to track — your security team and leadership should work together to choose the benchmarks that matter most to your organization based on your business goals, best practices, and your company's specific risk. (You may also choose to use competitors' best practices and security budget as a KPI, for example.)

These KPIs should be easy to obtain, easily measurable, and easy to understand.

What are the challenges of cybersecurity performance management?

Although metrics are key, they can also be a distraction. If you're tracking too many metrics, or if your KPIs are subjective or irrelevant, the story you're trying to tell about your cybersecurity program can get distorted.

McKinsey's James Kaplan and Jim Boehm offer the example of reports sent by the security team to senior management. Those reports feature references to "the millions of attacks the organization faces per week or per day." While "millions of attacks" sounds impressive, those incidents are likely not from skilled cybercriminals, and are probably pretty easy to repel.

Focusing on just the number of deflected incidents can provide management with a false sense of security. Executives might think they've got a robust cybersecurity program — after all, they're catching and resolving millions of attacks a week — when in fact the real threats are flying under the radar.

Another pitfall in cybersecurity management is static reporting. Organizations may be relying on metrics that are only issued periodically, such as point-in-time assessments. Those reports are snapshots capturing just one moment. A vendor that's in compliance when a questionnaire is filled out may be out of compliance the next day.

Benefits of security performance management

Security performance management provides a baseline for improving an organization's security, helps an organization make the most cost-effective decisions, increases cybersecurity return on investment, and enables leaders to efficiently utilize resources where they are needed most. It also helps connect members of an organization and facilitate conversations between the CISO, C-suite and board.