INFORMATION SECURITY: CYBER CRIME

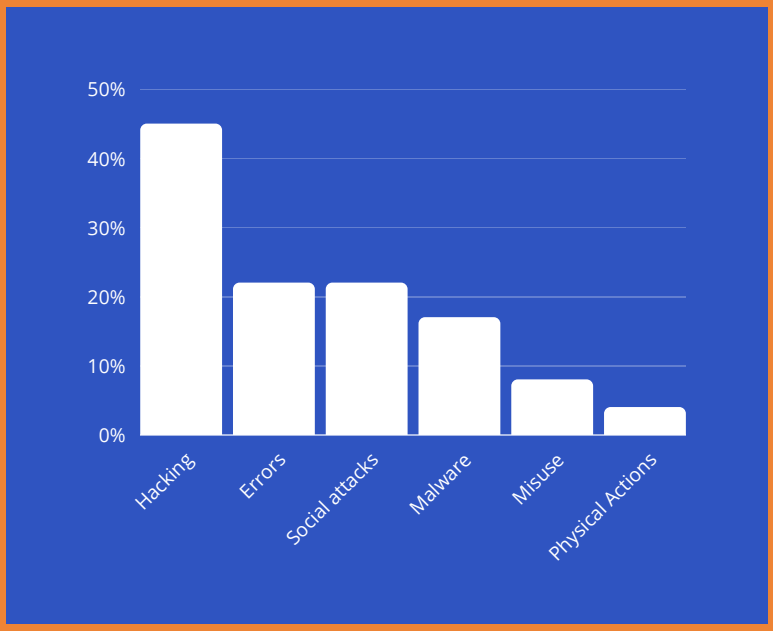
WHO IS ULTIMATELY RESPONSIBLE FOR A CYBER INCURSION?

Hint for Board Members: It is not your IT department.

WHAT'S INSIDE

Steps Board members can take to protect their organization
Choosing the right information security framework
Considerations for efficient security management & compliance

EXTEND RESOURCES



TACTICS USED TO GENERATE DATA BREACHES

While social engineering and malware are on the rise, the latest evaluation of data breaches shows that hacking remains the tactic most commonly used by cyber criminals to breach an organization's data.

Source: Verizon 2020 Data Breach Investigations Report

INTRODUCTION

2020 will go down as the year when businesses experienced massive increases in hacking activity, data breaches, and ransomware attacks. Many US and international organizations, including those that provide crucial education, healthcare, legal, retail and financial services, have been victims of such cybercrime.

WHY ARE CYBER-ATTACKS INCREASING?

First, COVID-19 and the resulting surge in remote work have both contributed to the increases. According to the Herjavec Group, “Since mid-January 2020, there has been an increase in COVID-19 related domain registrations. Attackers register new domain names containing wording related to coronavirus or COVID-19, which are then used in phishing campaigns to distribute malware.”

Additionally, as COVID-19 caused organizations to shift employees to remote work, malicious actors are exploiting publicly known vulnerabilities in VPNs and other remote working tools and software to introduce malware and/or gain access to confidential data and meetings.

Data published by CrowdStrike in their 2020 Global Threat Report identified that ransomware has also taken 2020 by storm.

Indeed, ransomware seems to pay very well. While there are still “independent contractors” across the world with access to cybercrime tools, more sophisticated criminals have begun to offer “Malware-as-a-service” (MaaS).

These developers, such as VENOM SPIDER, have created programs that will educate potential hackers and provide them with the tools they need to hack and charge ransomware fees.

WHY SHOULD BOARDS OF DIRECTORS PAY ATTENTION?

The Information Technology (IT) team often takes the fall when a data breach or security incident occurs. And cybersecurity professionals who experience a data breach on their watch will definitely be in the crosshairs.

However, the Board of Directors maintains ultimate responsibility for ensuring the companies they serve are properly managed and have the appropriate technology, processes, and personnel in place to protect their sensitive data.

Of course, the vast majority of company Board members are not data security experts; they bring other very significant business expertise to the table.

They must rely on the company's internal resources, typically a Chief Information Security Officer (CISO), or outside consultants to provide guidance and insight to ensure they meet their obligations to the company and their customers.

PROTECTING THE ORGANIZATION

WHAT STEPS SHOULD BOARD MEMBERS TAKE?

Just as the Board evaluates financial reports and legal matters each month, they should also assess the organizations' cybersecurity program health. They need to be aware of and understand identified security and privacy risks, the plans to mitigate those risks, and the status of tasks to treat identified risks.

Like they do for other vital departments, they should require associated KPI data and operational reports on information security management and compliance.

To meet the cyber-crime threats and demonstrate the fulfillment of their duty to the company, a Board of Directors should commit to the strategies outlined here.

Put information security at the top of the agenda.

If your company cannot operate because it is under a ransomware attack, the remaining agenda topics will not matter.

Dedicate time on the regular meeting agenda to discuss the current information security status. Include reports and relevant information in pre-meeting material, so the Board is prepared to discuss and understand the current information security environment and any potential issues.

Elevate your information security chops.

When it comes to protecting information, tone from the top is critical.

The Board should include a member who takes responsibility for cybersecurity. If this is not feasible, one or more of the board members should commit to becoming the information security leads, working closely with the organization's infosec team to gather and help communicate operational updates. This activity is more involved than meeting with the IT department personnel responsible for keeping the day-to-day technology solutions up and running.

Amplify awareness and involvement.

To create a healthy security posture, you must step back and ask the difficult questions.

The member(s) leading cybersecurity at the board level will need to understand and oversee various tasks, including defining the company's infosec goals and risk appetite, ensuring that security requirements are defined and monitored, and obtaining cybersecurity monitoring technology. Additionally, they should be notified immediately of any security incidents that occur, monitor auditing and awareness campaigns, and be aware of or involved in regular table-top or scenario-based exercises.

Choose the right security framework or standard.

Your industry, regulatory environment, operations, location(s), client requirements, and goals drive framework selection.

The Board should be involved in deciding which framework or standard the company will use as a set of best practices to manage its information security and privacy programs. Each company is unique and may be subject to various compliance requirements based on its location or industry.

Engage in a full risk assessment.

If you are not aware of a security gap today, there is a good chance it will grow into a perilous chasm.

Risk assessment, a foundation of a reliable security management program, identifies the information assets that could be affected by a security incident (such as hardware, systems, laptops, customer data, and intellectual property). Throughout, assessors document potential weaknesses for that asset type, evaluate risk levels associated with those assets based on an organization's unique needs, and outline how the risk may be mitigated.

INFOSEC FRAMEWORKS: MAKING THE RIGHT CHOICE

There are a variety of guidelines companies can use to create and manage an information security program. Frameworks are guidelines for managing a program. Standards are a set of requirements that offer certification. See the most commonly used frameworks and standards below.

Selecting the right options should be based on the needs of the company. An organization may need to meet the requirements of more than one framework.

Companies based outside the US or that have international locations may choose a different framework than a company that only does business in the US. Healthcare organizations or companies that work with protected health information (PHI) may need to comply with HIPAA guidelines in addition to an infosec standard.

Check with your attorney and CISO to determine what standards your organization will need to use.

NIST CSF

The National Institute of Standards and Technology (NIST) provides standards for recommended security controls for information systems at federal agencies. This framework is used in many US-based companies.

ISO 27001

This standard can be used to certify the quality of an information security program used by US and international companies. The International Organization for Standardization also recently published the ISO 27701 standard for data privacy.

CTPAT

The Customs Trade Partnership Against Terrorism is a cargo enforcement program from the US Customers and Border Protection agency. If a company is CTPAT certified, its incoming international goods will be expedited through Customs.

GDPR

General Data Protection Regulation, a legal framework for collecting and processing personal information from those that live in the European Union (EU). Companies that provide goods or services to the EU may need to meet this standard.

CCPA & SIMILAR STATE LAWS

California recently implemented the California Consumer Privacy Act and other states may follow its lead. The law requires organizations to obtain consent from individuals to collect and use their data and to disclose how the data is used.

HIPAA

The Health Insurance Portability and Accountability Act is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. If your company has access to Protected Health Information (PHI), you may be subject to HIPAA regulations.

EFFICIENT SECURITY MANAGEMENT & COMPLIANCE

Securing and protecting an organization's information assets is a lot of responsibility. Success takes more than a simple commitment; it takes an organized, disciplined approach. Just as organizations use financial software to manage their accounting activities, efficient, cost-effective information security programs rely on proper management software to track performance and generate results.

Your CISO, who has operational responsibility for protecting information assets, should have a platform specifically designed to manage security.

The platform should serve as a single repository where the entire program – policies, assessments, mitigation plans tasks, training records, and risk management and audit activities, and scorecards – are managed.

Choosing the right platform will enable your organization to avoid the many time-consuming, expensive obstacles that often come with using spreadsheets and home-grown collaboration tools to handle such a complex process. Consider these capabilities when looking for compliance management software.

KPI Reports

Track your security posture performance, including the status of mitigation activities, for the executive team and the Board.

Risk Assessment

Calculate the risk associated with each asset and how that risk is managed – Accepted, Avoided, or Transferred. It should be easily updated and maintain a history of updates for auditing purposes.

Stakeholder Collaboration

Work as a team during table-top exercises and other cybersecurity team discussion sessions. Table-top exercises, where members meet and discuss their incident management roles in a low-stress, scenario-based activity, are required periodically to maintain accreditation.

Vendor Risk Management

Efficiently evaluate your vendors' and partners' security posture with questionnaires and communication tools.

Document Library

Enhance efficiency by using a pre-drafted set of customizable policy templates. Managing program documents in one repository ensures version control and easy access for review and audits.

Auditor-Friendly Collaboration & Reports

Unique views and collaboration tools that deliver easy access to required information, provide space where an independent auditor can use to insert their notes, comments, and documents regarding their findings, and help them validate compliance and streamline audits.

A NOTE ON THIRD-PARTY AUDITING

Whether internal, client-based, or performed by a third-party auditor for certification purposes, information security audits can be very complex and require significant documentation to confirm that a program meets objectives and sufficiently protects the company's assets. Just as an organization periodically audits its financial records, auditing the information security management system is key to validating that the security policies, procedures, and documentation follow recognized guidelines. Not only is an independent audit key to the program's ongoing success, but it is also required to maintain proper certification offered by some frameworks.

Using a compliance management platform that includes documentation to support the program and audits will streamline the audit process by providing the auditor with easy to find supporting documentation.

Should a cyber incursion or incident occur, documenting the company's efforts to maintain good cyber hygiene is essential. Fines for companies that have implemented tight information security controls may be less than a penalty imposed on a company that does not have a well-documented cybersecurity program.

IN SUMMARY

The Board of Directors is responsible for ensuring the company's cybersecurity and information privacy program meets or exceeds the standards set out by its industry, company, and clients.

It is incumbent on the directors to understand information security best practices and question the company's executives and information security officers to ensure that the organization's security posture is maintained at a high level.

Using compliance software designed for information security programs is essential to properly managing the program and ensuring that an organization meets its goals.

In addition to providing a disciplined workflow for the cybersecurity team to manage and document their processes, a full-featured platform enables the Board to view operational KPIs and ensure the program continues to comply with national, international, and other standards.

EXTEND RESOURCES

T/F (203) 479-9408
info@extendresources.com

1127 High Ridge Road, Suite 170, Stamford, CT 06905
V20201125