NETENRICH

A BOARD'S-EYE VIEW OF CYBERSECURITY RISK

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

TABLE OF CONTENTS

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

Cybersecurity has entered the board room

Major cybersecurity events are in the news daily, and many more events never make the news. The impact and costs to businesses and communities mean that corporate boards must consider cybersecurity risks among key business risks.

Cyber breaches cause extensive damage and can put companies out of business. Yet there are ways to reduce these risks and damage.

It's the chief information security officer's (CISO's) job to communicate about cybersecurity risks so that their boards understand these risks in a business context. Yet, most board members don't have the technical background to understand the details of what's happening in your Security Operations Center (SOC). They do understand management of business risk, so it's critical to frame cybersecurity risk within a business context: consider the impact on budgets, stock price, and brand perception. This guide helps CISOs, CIOs, and their boards to manage cybersecurity risk and, in the process, reduce exposure to harm.

Cybersecurity is a strategic business risk

Recent cybersecurity disasters prove that boards and executive teams must treat cybersecurity as a strategic business risk, well beyond the scope of compliance and regulations. Cybersecurity impacts business growth, business continuity, brand reputation, customer trust, and business relationships.

According to the IBM Security/ Ponemon Institute *Cost of a Data Breach Report 2023* based on **553 organizations** across **16 countries** and in **17 different industries:**

204 is the average number of days to identify and contain a data breach. The longer it took to identify and contain, the more costly the breach.

$332 million is the average cost of a mega breach (between 50 million and 60 million records).

$4.45 million is the global average total cost of a data breach.

$5.13 million is the average cost of a ransomware breach. Ransomware and destructive attacks are the most costly types of breaches.

Companies that fully deployed security AI and automation **reduced their breach costs by 66%** compared to companies that did not deploy security AI and automation.

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

> ***Asking the smart questions at your next board meeting might just prevent a breach from becoming a total disaster.[1]***

According to the **National Association of Corporate Directors (NACD)**, "Cybersecurity is now a major strategic and enterprise risk matter that affects how companies operate, innovate, and create value. Several characteristics combine to make the nature of the threat especially formidable: its complexity and speed of evolution, the potential for significant financial, competitive, and reputational damage, and the fact that **total protection is an unrealistic objective.**"

Total protection in a world connected by the internet and run by software and humans is impossible. Hence the importance of a risk-based, business-aligned approach to managing cybersecurity.

Audits and regulatory reports aren't enough

Today's audits and most regulatory reports emphasize controls and criteria established by frameworks such as those from the International Organization for Standardization (ISO) and the U.S. National Institute of Standards and Technology (NIST). But it's not enough.

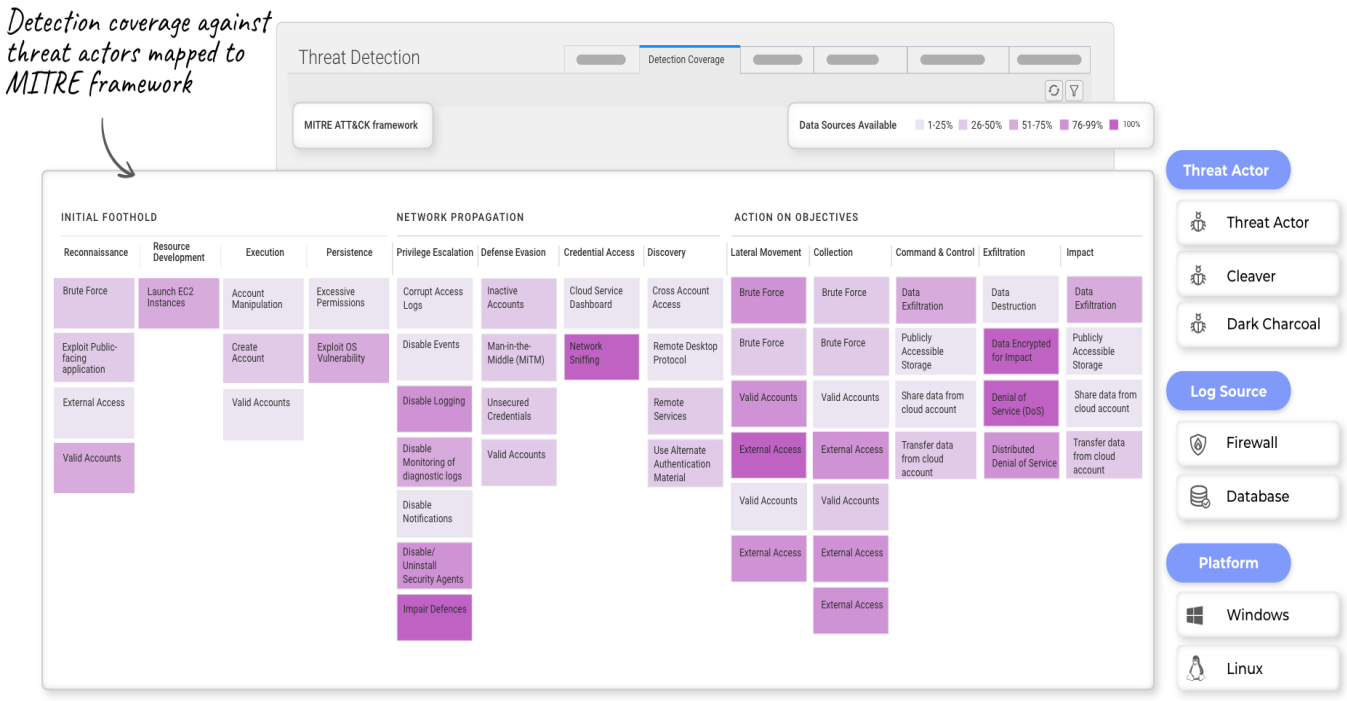
Checking boxes for compliance reports further implies that the answer to "are we safe?" that's a yes or no answer — but it doesn't. Like all business risk, you can't make cybersecurity risk go away. You can be prepared and choose where to mitigate it based on costs and benefits.

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

Understand where you are vulnerable

MITRE | ATT&CK®

MITRE ATT&CK® is a publicly accessible knowledge base of cyber adversary behavior and taxonomy for adversarial actions across their lifecycle. ATT&CK® takes an attacker's point of view to help organizations understand how attackers approach, prepare for, and execute attacks. The taxonomy can be used to understand the "foot print" of known, real-world attacks and to identify where your organization may be at risk, as shown below in a screen shot from Resolution Intelligence Cloud™ from Netenrich. The lighter grey boxes highlight areas with insufficient detection coverage. The darkest purple boxes show areas of 100% coverage.



 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

Use a risk-based approach to cybersecurity

A risk-based approach to cybersecurity is especially important as digital operations expand and become more complex, through remote workforces, public cloud exposures, mergers and acquisitions, digital transformation, and more.

CISOs and CIOs should identify and update their boards on the business risks of critical cybersecurity issues on a regular basis with:

- Identification of and plans for protecting business-critical assets and data.
- Potential cybersecurity events most likely to occur given recent events, your industry, known vulnerabilities, changes to the digital landscape such as acquisitions, etc.
- Probability of occurrence of these events (this is typically estimated using historical data and industry data from peers).
- Potential impact and cost if an event occurs.
- Cost to reduce the impact of or avoid a potential event.

Focus efforts and resources on minimizing the most dangerous risks in the most cost-effective ways that meet your business's risk tolerance, such as:

- Implementing attack surface management (ASM) and threat research strategies to better identify and address vulnerabilities proactively.
- Focusing on detecting patterns of risky behavior that are most relevant to your company, industry, and known exploits.
- Identifying key assets and data that are most critical to the business and reduce their vulnerabilities on a frequent basis.

According to Harvard Business Review, boards of directors need to know these five things about cybersecurity[1]:

1. Cybersecurity is more than protecting data.
2. The BODs must be knowledgeable participants in cybersecurity oversight.
3. Boards must focus on risk, reputation, and business continuity.
4. The prevailing approach to cybersecurity is defense-in-depth.
5. Cybersecurity is an organizational problem, not just a technical problem.

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

- Automating routine tasks to reduce toil and refocus efforts.
- Improving risk management by using advanced data analytics and machine learning algorithms to monitor and tune processes and systems.
- Continuously measuring multiple metrics and looking at historical trends to improve data quality and adapt workflows.

Siloed digital operations obstructs risk-based cybersecurity

Unfortunately, most CISOs do their jobs in a context that impedes their success. SOCs are isolated from overall digital operations and focus on resolving any sign of a potential incident. Yet doing so they are likely to miss the big picture. The proliferation of security tools has led to the need to hire more experts to run them, yet cybercrime is on the rise and there's no end in sight.

Given that total protection is impossible, SOCs need to align management of cyber risk with the business, with the goal of delivering secure operations to the business. When a breach occurs, no one will be impressed with how many security tools and experts you have.

> ***Cyber risks cannot be managed in silos, fragmented among specific individuals or departments (e.g., IT department, finance team, legal, etc.) responsible for a piece of an organization's risks with little or no in-between interaction. By leveraging data from entities within and outside their circle, organizations can fully realize the possible extent of their vulnerabilities (if exploited), such as to other sectors or industries; identify clusters of common vulnerabilities and drivers of risk; and evaluate investments in cyber controls to holistically and collectively manage these risks."*** [2]

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

Most tools, activities, and intelligence in a traditional SOC focus on threat detection versus exposure to and risk from potential threats. Indications of potential of malware, active exfiltration, and/or insider attack appears and sets off a chain of events to find, validate, and neutralize or contain the threat.

- The traditional, threat-centric approach to the SOC isn't efficient or sufficient.
- Disparate tools produce too many alerts for security teams to manage, and they have no idea which alerts matter most.
- A tsunami of noise and false positives obscures serious threats and risks.
- Disjointed manual processes take too much time and effort.
- More tools require more experts to manage them — and it's challenging to hire and keep them.

Focus on secure operations

Focusing on secure operations is a strategic shift to viewing cybersecurity risk holistically in terms of threats and exposure. It requires takes a multi-layered approach to making security operations more effective and your security posture stronger across all digital operations.

CISOs and CIOs focus on CIA: confidentiality, integrity, and availability. Boards of Directors are concerned with risk, reputation, and business continuity. Working together, they can manage cybersecurity as a business risk and reduce exposure to harm.

A more agile, dynamic approach is needed, and it's here

Netenrich boosts the effectiveness of organizations' security and digital operations so they can avoid disruption and preempt risk. Our Resolution Intelligence Cloud is a secure analytics operations platform that turns complex big data into actionable intelligence so enterprises can expose and manage security risk to reduce business impact. Leveraging advanced security analytics and machine learning, the agnostic platform transforms security and ops data into

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023

intelligence that organizations can act on before critical issues occur. More than 3,000 global customers rely on Netenrich to increase operations efficacy while scaling to meet the needs of the business.

Manage cybersecurity as a strategic business risk

Schedule a secure operations assessment with a Netenrich security expert and learn how Resolution Intelligence Cloud helps you manage and minimize cybersecurity risk exposure.

Visit **www.netenrich.com**

About Netenrich

Netenrich makes data the solution, not the problem. With Resolution Intelligence Cloud, our secure analytics operations platform, we turn complex big data into actionable intelligence so enterprises can expose and manage security risk to reduce business impact. The platform leverages a cybersecurity mesh architecture (CSMA) to converge security and digital operations. Its data engineering, multitenant, and automation (AI, ML) capabilities improve current security systems, for more accurate threat management and response. More than 3,000 global customers rely on Netenrich to increase operations efficacy while scaling to meet the needs of the business.

[1] Dr. Keri Pearlson and Nelson Novaes Neto, "7 Pressing Cybersecurity Questions Boards Need to Ask," March 04, 2022, **hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask**

[2] **Systemic Cyber Risk Reduction**

 © 2023 NETENRICH, INC. ALL RIGHTS RESERVED. v.02062023