Managing cybersecurity risk needs to go beyond a preventive mindset

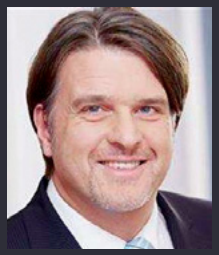
Legal, Compliance and Technology Executive Series

EY
Building a better working world

Of special interest to:

Legal counsel
Corporate security officers
Information security executives
Compliance executives
Risk management executives
Internal audit

Author:



Bodo Meseke

Partner, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany

Introduction

The primary strategy for defending an organization from the risks of cyber attacks has long been prevention — stopping attacks before they are successful. But the growing sophistication of cyber criminals has made it very difficult to completely stop breaches from occurring. One breach that is discovered too late can cost millions of dollars, cripple operations and even put companies out of business.

> It's estimated that US companies lost $654 billion to cyber attacks in 2019, with nearly 60% of organizations facing a material or significant incident over the past year, according to the EY Global Information Security Survey 2020.[1]

Hackers hoping to exploit fears amid the COVID-19 crisis are increasingly resorting to phishing and ransomware attacks. The International Criminal Police Organization (INTERPOL) has detected a significant increase in ransomware attacks against hospitals and other health care providers around the world.[2] Cyber criminals are also increasingly targeting mobile devices, a trend that is likely to worsen as remote workers turn to their phones to conduct business. More than half of IT leaders surveyed in 2020 said mobile devices are very or extremely challenging to defend.[3]

1 Kris Lovejoy, "How to manage cyber risk with a Security by Design approach," EY, 7 February 2020, https://www.ey.com/en_gl/advisory/how-to-manage-cyber-risk-with-a-security-by-design-approach.

2 "Cybercriminals targeting critical healthcare institutions with ransomware," *INTERPOL website*, 4 April 2020, https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

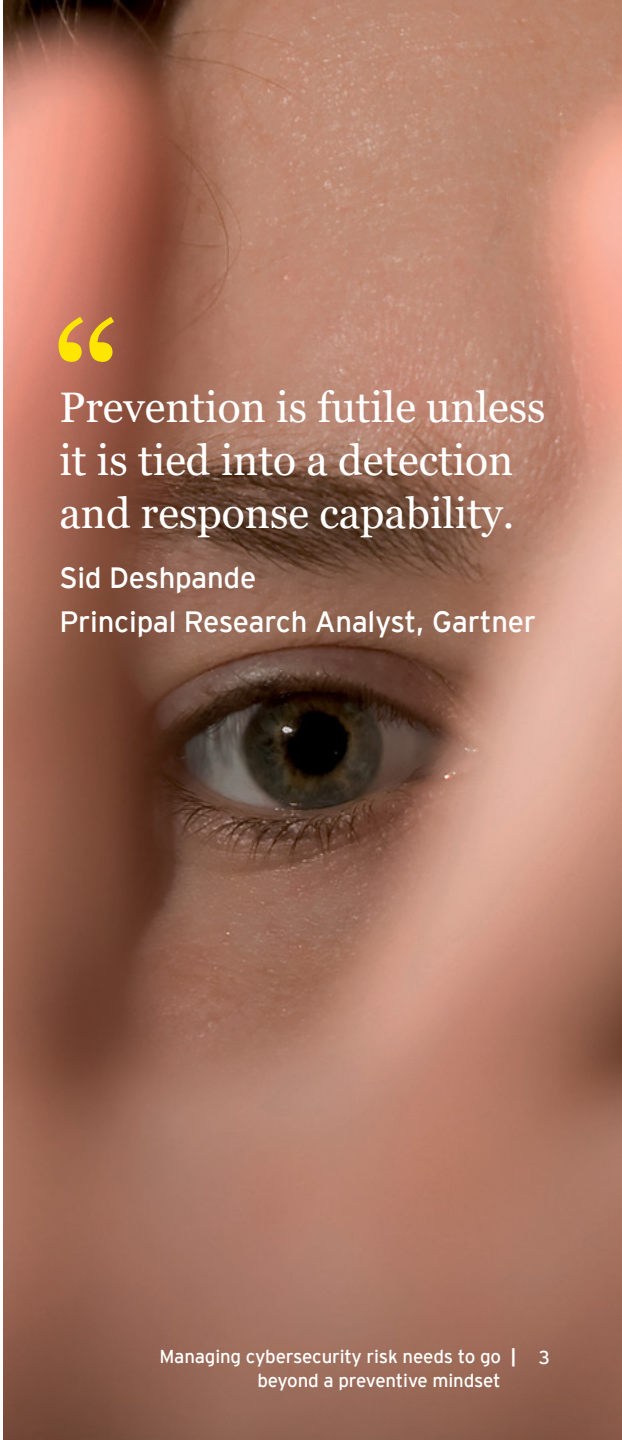
3 *Securing What's Now and What's Next*, Cisco 2020 CISO Benchmark Survey, Cisco, 24 February 2020.

Prevention alone isn't enough

Even the best defense isn't criminal proof, with attacks becoming increasingly sophisticated. Criminals are even weaponizing artificial intelligence (AI). For example, hackers can create intelligent malware programs that learn from thwarted attacks and create modifications that make subsequent attacks successful.

Eighty percent of IT professionals surveyed in 2020 said prevention is the most difficult aspect of cybersecurity due to insufficient technology, lack of in-house expertise and the time needed to identify threats.[4] More than three-quarters of respondents agreed with this statement: "*My organization focuses on the detection of cyber attacks because prevention is perceived to be too difficult to achieve*."

While prevention will continue to be important in cybersecurity, organizations are increasingly realizing they can reduce risk and damages by prioritizing rapid detection of threats and effective incident response.



> "Prevention is futile unless it is tied into a detection and response capability.
>
> **Sid Deshpande**
> **Principal Research Analyst, Gartner**

4 *The Economic Value of Prevention in the Cybersecurity Lifecycle*, Ponemon Institute and Deep Instinct, April 2020.

Delay in detection and response has been a persistent issue

Reacting effectively to a breach requires both a response team and a plan that is continually honed with tabletop exercises or cyber simulations.

Organizations that conducted extensive testing of an incident response plan reduced the average cost of a breach by more than $1 million compared to organizations that failed to form a breach response team or test a plan.

Source: *Cost of a Data Breach Report 2019*, Ponemon Institute and IBM Security

Medical professionals use a concept called the *golden hour* to describe a short period of time following a traumatic injury during which prompt medical treatment has the greatest opportunity to minimize ultimate damage. In a similar way, cybersecurity professionals also have a limited window of time to detect and contain attacks before they cause serious harm to an organization.

A 2019 Verizon investigation into thousands of security incidents found more than half of all breaches took months or longer to discover.[5] For example, payment card compromises aren't usually discovered until the stolen data is used, which typically takes weeks or months. The mean time for identifying and containing a breach caused by a malicious attack was 314 days, according to a 2019 report.[6]

Delays in responding to breaches give attackers time to steal or manipulate data, greatly increasing damages. Even larger costs can be incurred from litigation, regulatory penalties and reputation loss. A large US retailer spent more than $200 million in legal fees and other costs, including an $18 million fine, for a data breach resulting from not thoroughly investigating software alerts. Major breaches can erode consumer trust and impact a company's revenues for years.

[5] *2019 Data Breach Investigations Report*, Verizon, May 2019. https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/.

[6] *Cost of a Data Breach Report 2019*, Ponemon Institute and IBM Security, July 2019, https://www.ibm.com/security/data-breach.

Significant false positives are a main cause of delayed detection and response

A primary reason breaches aren't detected sooner is the sheer volume of security alerts that overwhelms security professionals. A global Cisco survey showed that 17% of organizations receive at least 100,000 or more daily alerts in 2020, compared to 11% in 2017. This led to roughly half of real threats being ignored.[7]

Security information and event management (SIEM) software is designed to help analysts by providing real-time monitoring of threats. But it's estimated that analysts spend roughly one quarter of their time looking into false positives generated from these tools.[8] A 2019 survey of cybersecurity professionals found it takes more than 10 minutes to investigate each alert, with roughly half eventually found to be false positives (mislabeled alerts that aren't actually threats).[9] As a result, analysts spend most of their time managing alerts rather than containing or remediating threats.

More and more SIEM providers are incorporating AI technologies to help reduce false positives. For example, Exabeam claims its machine learning SIEM platform results in a false positive rate of just 10%.

7 *Securing What's Now and What's Next*, Cisco 2020 CISO Benchmark Survey, Cisco, 24 February 2020.
8 *Exabeam SIEM Productivity Study*, Ponemon Institute and Exabeam, July 2019.
9 *The Impact of Security Alert Overload*, Critical Start, August 2019.

Intelligent automation becomes essential for rapid detection and response

As the volume of threats rises, more organizations are combining automation with AI to detect and respond to attacks more efficiently. Organizations without security automation suffered almost double the costs from a breach than organizations with fully deployed automation in 2019.[10] And 75% of security professionals surveyed in 2019 said automation is highly valuable to achieving cyber resilience.[11]

AI tools can be programmed to block threats automatically or outmaneuver them by sending false signals as they gather information. When a new type of malware appears, AI tools compare it to previous forms in their databases and decide if it should be automatically blocked. Machine learning can evolve to recognize ransomware before it encrypts data and can determine whether a website navigates to a malicious domain. The most effective type of threat detection incorporates both AI and humans. Organizations using AI say they've reduced the time taken to detect threats and breaches by 12%.[12] AI can also improve user authentication and password protection.

[10] *Cost of a Data Breach Report 2019*, Ponemon Institute and IBM Security, July 2019, https://www.ibm.com/security/data-breach.

[11] *The Cyber Resilient Organization*, Ponemon Institute and IBM Security, April 2019.

[12] *Reinventing Cybersecurity with Artificial Intelligence*, Capgemini Research Institute, July 2019.

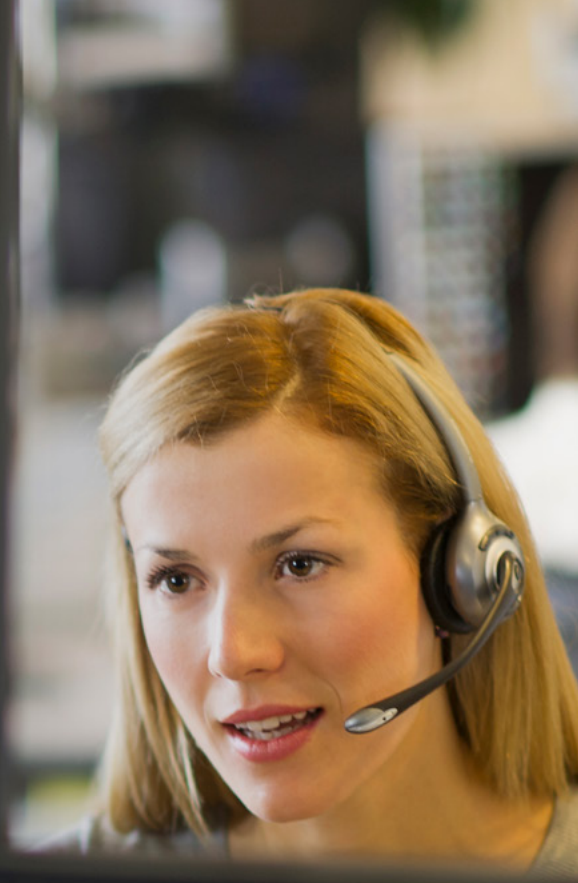
Using SOAR to manage alerts and improve response

Many organizations are now turning to security orchestration, automation and response (SOAR), technologies that use data from SIEM and other security systems to standardize and shorten incident response processes. SOAR combines orchestration, automation, threat intelligence, and human and machine learning to detect and contain threats.

SOAR analyzes each security incident and decides whether to act automatically or request human intervention. For example, SOAR can isolate or shut down a system instantly if malicious activity is detected. It also can slow the spread of malware by automating actions like forensic data gathering and running vulnerability scans. Automated orchestrated incident response saves an average of $1.5 million in data breach costs, according to IBM.[13]

[13] "Orchestrate incident response," *IBM Security website*, https://ibm-security-solutions-orchestrate-incident-response-ebook.mybluemix.net/?cm_sp=CTO-_-en_US-_-LNRYV2MP

Outsourcing threat detection and incident response



Small to midsize organizations may be unable to invest in the technology or human resources needed to quickly detect and respond to security incidents. Small businesses, public sector agencies and health care providers have been increasingly targeted by cyber criminals who are finding greater success with soft, data-rich targets. At minimum, all organizations should be vigilant about installing and continually updating antivirus and anti-malware programs. Having a sufficient number of well-trained security professionals is also critical for quickly detecting threats and preventing unauthorized access.

Many organizations are finding outsourcing security to be their best solution, but care must be taken to choose a reliable vendor. Roughly one-third of organizations surveyed by Cisco in 2020 outsourced incident response services, with more than half citing *more timely response to incidents* as the main reason why.[14]

Managed detection response (MDR) is becoming an increasingly popular option, especially for smaller organizations. MDR is a service that detects malware and malicious activity, and assists organizations in responding rapidly to eliminate those threats. MDR typically combines technology with outsourced analysts. Gartner predicts that by 2024, a quarter of organizations will be using MDR services, up from just 5% in 2019.[15]

[14] *Securing What's Now and What's Next*, Cisco 2020 CISO Benchmark Survey, Cisco, 24 February 2020.

[15] *Market Guide for Managed Detection and Response*, Gartner Research, 15 July 2019.

In summary

While prevention will always be an essential part of a successful cybersecurity program, odds are an organization will be victimized at some point. When that happens, the best way to lessen the impact is through quick detection and effective containment. This will help reduce the risk of regulatory penalties, costly litigation and reputational damage.

Organizations should understand that managing cyber risk requires a strategy that extends beyond prevention. A proactive stance on cybersecurity is a core tenet of the EY Security by Design approach, which looks beyond protection to manage and mitigate security risks.

Security by Design

Security by Design is a proactive and strategic approach that considers cyber risk and security from the onset of any new initiative, rather than as an afterthought.

This approach focuses on enabling trust in systems, designs and data so organizations can take on more risk and innovate with confidence. For example, appropriate data governance, identity and access management protocols must be implemented into AI systems to prevent outcomes from being corrupted.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYG no. 003051-20Gbl
WR #2004-3472420
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com