WHITE PAPER

Malwarebytes

HOW TO BECOME CYBER RESILIENT:

A Digital Enterprise Guide

June 2019

Introduction

> Digital transformation has revolutionized the way businesses operate, providing a foundational shift in how they meet market demands and deliver value to customers. At the same time, it has created an explosion of data and endpoints, with the proliferation of mobile and IoT devices. Both require vigilant protection from cyberattacks.

Strong cybersecurity has always been an essential component of a company's digital transformation success. However, traditional practices of securing data with fixed firewalls and signature-based antivirus solutions in a world of polymorphic attacks and mobile workforces are simply not enough. The constant expansion of attack surfaces has made protection more difficult and a successful attack more inevitable. In fact, according to a 2019 Malwarebytes cyber resilience study of over 350 security professionals, 75 percent of organizations assume they are likely to experience a breach within the next one to three years.

As a result, organizations are reexamining their investments to build a security posture of resilience. Building cyber resiliency requires organizations to evaluate their people, processes, and technology to ensure they have the best protection in place and can operate during a cyberattack, as well as quickly recover from it. A lack of cyber resiliency can lead to astronomical costs—ranging from closure for small businesses to seismic operational disruptions for larger enterprises. A single breach can add up to US$4.2 million in lost business stemming from customer turnover, increased customer acquisition activities, reputation losses, and diminished goodwill.[1]

To apply weight to this goal, corporate executives and board members are increasingly asking CISOs to present their cyber resiliency strategy and assume responsibility for seamless execution of the plan. The Malwarebytes study on resilience found that over 87 percent of security professionals are required to discuss security response plans with their executives and Board at least once per year. CISOs, therefore, must be ready to demonstrate that they have established a posture of cyber resilience—one that not only protects the company's data, endpoints, and operational functionality, but also ensures continued business growth.

This paper, then, explores the current market influences that impact how an organization pursues cyber resilience, the key methods that should be adopted in becoming cyber resilient, and the reasons why cyber resilience can transform an organization into a digital enterprise highly focused on growth.

Trends driving endpoint exposure

Undoubtedly, the way companies conduct business has changed significantly in recent years. Business-enabling technologies and systems, such as collaboration tools, BYOD, and cloud services have been innovating at a breakneck pace. As a result, IT has needed to continually redefine its strategic focus to adapt. Amid this disruption, companies are experiencing the convergence of pivotal market trends that have made the endpoint the new perimeter, creating a business imperative to prioritize cyber resiliency.

Expanding attack surface

A key trend driving the need for cyber resiliency is the expanded corporate attack surface stemming from cloud adoption and device mobility. With the introduction of cloud computing, businesses quickly saw the value and opportunity to offload infrastructure investments and scale resources. IDC predicts that 67 percent of enterprise infrastructure and software will be for cloud-based offerings by 2020.

However, cloud adoption and mobile-enabled employees have introduced distributed networks, which are more complex to secure, and consequently, cybercriminals have been given more avenues whereby they can dole out their attacks on companies. Consequently, the expanded corporate attack surface has created one of the greatest pressure points for companies to establish cyber resiliency.

Increasing value of data

The advancement of digital transformation and artificial intelligence, as well as the use of big data has led to the rise of insight-driven business—one where data empowers growth through market disruption, enabling productivity and opening new revenue streams. Across industries, companies have evolved so that the data they hold is, in fact, their flagship product. Indeed, 63 percent of senior decision makers report that big data is now a driver of revenue and is becoming as valuable to their businesses as their existing products and services.[2]

The value of corporate data hasn't gone unnoticed by cyber criminals. With stolen personal information, they can earn US$1,000 per record on the black market,[3] as well as commit social engineering scams and a variety of other illegal acts. Accessing that highly-sought-after data is the driving force behind cyberattacks on corporate networks, which relentlessly pursue employee endpoints to gain a foothold into the organization.[4] With 70 percent of companies reporting that their data is very to critically important to the business operations,[5] cyber resilience becomes essential for organizations to ensure that their data is safely protected and accessible at all times.

Ever-evolving attacks

Since the dawn of the first cyberattack, threat actors have continually advanced their tactics to evade detection and gain access to corporate endpoints. Originally, attacks on endpoints were launched merely as a pathway into the enterprise network for more valuable targets. In recent years, however, automated attacks like ransomware and laterally

spreading exploits, such as SMB vulnerabilities have "democratized" the victim pool, making the endpoint itself, and the data on it, the prime target.

And companies of every size are in the fray. Cybercriminals have created dark web marketplaces that provide an ecosystem for their peers to collaborate and build sophisticated attack packages at minimal expense. This, in turn, has made it viable for threat actors to broaden the scope of their targets and pursue businesses of all sizes. And just one successful attack can disrupt operations and occupy response teams for weeks to successfully restore the network.

Complex and increasingly punitive compliance requirements

Regulations have been a necessary component of the digital age to provide legislative guardrails that ensure companies are adopting adequate care to safeguard their customers' sensitive data. Now, more than 100 countries around the globe have enacted comprehensive data protection legislation.

Between far sweeping, international regulations such as the Global Data Privacy Regulation (GDPR), industry-specific compliance frameworks, and state-level legislation, most organizations across industries must comply with some level of regulation. And often, companies are impacted by multiple, differing regulations.

The ever-changing regulatory environment has created an increasingly complex compliance labyrinth for organizations to navigate. Yet, noncompliance can lead to steep fines, as well as result in corporate operations that are unable to perform with agility and exactness when an incident occurs.

Increasing costs of breaches and mitigations

Successful breaches cost organizations significantly in lost revenue, customer turnover, and data loss. And it's hard for companies to recover from interruptions to operations and reduced brand value. Think back to the 32GBs hackers published in July 2015, exposing personal details on Ashley Madison's entire customer base when the company refused to pay a demanded Bitcoin ransom. As part of the fallout, users whose details were leaked won a class-action lawsuit against the company for US$11.2 million.[6]

The cost of breaches and mitigations are on the rise. According to Ponemon Institute, the average breach has skyrocketed to 24,615 records globally and costs US$3.8 million.[7] If the costs of a breach don't put a company out of business, often, it can take years for the organization to recover and return to their same level of financial performance.

These converging trends have pushed the corporate endpoint forward as the new first line of defense against security breaches. In addition, they are creating greater urgency and importance on an organization's readiness to deliver effective cyber resilience in the face of the inevitable attack.

Challenges of achieving cyber resilience

For CISOs, building enterprise resilience is a Board-level requirement. However, putting resilience into action has posed significant challenges. One-third of security professionals lack a response plan for security breaches, which means that when these organizations get attacked, they will be slow to recover. This is in an environment where over three-quarters of organizations believe they will be targeted and will experience a breach within the next three years.[8]

This represents a high-risk gap between resilience planning and a CISO's readiness to deliver on the plan. The extensive difficulties in achieving a cyber-resilient organization move across the cybersecurity pillars of an organization's people, processes, and technology.

Skills shortage in face of increasing complexity

Having knowledgeable staff with strong security expertise continues to present challenges with 56 percent of organizations reporting an inability to hire and retain skilled staff.[9] Unfortunately, this is a systemic problem with no end in sight. According to Cybersecurity Ventures, there will be 3.5 million unfilled cybersecurity positions by 2021.

With ever-evolving threats, the pervasive shortage of cyber security resources and skills presents a daily challenge for CISOs who need to constantly train staff to keep up, as well as navigate the operational complexities of attracting candidates to fill open positions.

Lacking inventory of key data and systems

Cyber resilience requires preparation by identifying and prioritizing the company's most critical data, endpoints, and systems that are essential for continued operations when an incident occurs. Yet, 46 percent of security professionals claim that their cyber resilience is impeded by a lack of visibility into applications and data assets.[10]

The main barrier: companies can't inventory what they can't see. With CISOs facing an expanded attack surface through cloud and device adoption, it is increasingly difficult to inventory what and where all the organization's data and shadow IT reside. Without this understanding, companies can't ensure all systems are adequately protected or apply rigor to their incident response methodologies.

Technology advancements and challenges

The advancements in business-enabling technologies has created an ever-changing digital environment for IT and security teams to manage and protect. Companies have adopted video collaboration platforms, joined the social media revolution, signed on for anything-as-a-service, and outfitted their employees with smart phones, just to name a few of the endless IT-enabled business trends.

In parallel, security technologies have changed and expanded with new controls entering the mix to shore up security gaps introduced by these business technologies, as well as innovating attacker methods. In fact, today's security operations center (SOC) infrastructure is comprised of at least 20 security applications.[11] Between business and security tools, there's a mountainous number of technologies IT is charged with mastering amid an environment that is constantly changing.

> **46%**
>
> of security professionals claim that their cyber resilience is impeded by a **lack of visibility into applications and data assets.**

Automation unlocks the key to cyber resilience

> Adopting a cyber resilience approach that covers the security framework from preparation through to response will minimize the impact of a cyberattack and ensure CISOs can act rapidly to restore systems and maintain business continuity. In the face of the enterprise challenges to achieve resiliency, organizations should identify where their cyber resilience is lacking across the framework and take steps to automate in shortfall areas.

Adopting automation mechanisms is an effective approach to strengthening cyber resilience, leading to better outcomes for security posture and delivering significant benefits. Companies that fully deploy security automation experience an average of US$1.55 million in incremental savings when handling a data breach.[12]

Automation is a way for CISOs to maximize their investment and relieve the pressure from continued staff and skills resource constraints. It's scalable, and it doesn't go to sleep. Automation also introduces a proactive security approach that can hunt for threats that might not be on the security team's radar.

Automate detection through AI and machine learning

A strong security posture is powered by strong threat intelligence. Automating threat intelligence using advanced analytics techniques, artificial intelligence, and machine learning gives organizations better threat detection capabilities to adapt as quickly as cybercriminals evolve their methods. In addition, these methods provide the best approach for detecting unknown threats.

Automating threat intelligence that applies advanced analytics at scale significantly increases detections of threats that previously slipped past corporate defenses, and, when done right, it also aids in reducing the noise from incident alerts and false positive rates from detection systems.

Companies are already recognizing the value of automated detection. According to the Malwarebytes study on resilience, 59 percent of security professionals have automated threat detection and 45 percent are planning to do more so in the future.

Automate response without impacting business

When a successful cyberattack occurs, it moves fast. Often, malware quickly spreads laterally from the first affected endpoint to other endpoints and systems in the environment. Companies are consistently facing resource and skills shortages that lead to long incident response times. On average, it takes companies 197 days to identify an attack and another 69 days to contain it.[13]

Investing in tools that automate response mechanisms can greatly improve a company's cyber

resilience. Requirements for automated response should include capabilities that allow organizations to actively respond to a threat, including the ability to automatically isolate, remediate, and recover.

Containing an attack is the first step in response. Incident response teams can plan remediation more effectively when an attack has been successfully isolated and prevented from doing further damage. For this reason, 47 percent of security managers have automated infected endpoint isolation and another 53 percent are planning to make near-term investments for automated endpoint isolation.[14]

Automated isolation should provide organizations with the flexibility to contain an infection while minimizing disruption to the user. This means containing a threat at the endpoint by isolating at the network, device, and process levels. These containment methods also impede malware from phoning home to receive command-and-control communication, which restricts it from doing further damage. Companies should also include recovery from ransomware attacks as a requirement of their automated response. This capability should include just-in-time endpoint backups that automatically wind back the clock and negate the impact of a ransomware attack.

The second requirement of a successful response is automated remediation. This bolsters a company's cyber resilience by quickly and effectively restoring systems without requiring staff resource time or expertise. In addition, it empowers CISOs to remediate endpoints at scale and to significantly reduce the company's mean-time-to-response.

The market is moving toward wide adoption of automated remediation with the removal of malware from endpoints. Fifty-four percent of security professionals report that they have adopted this capability in their cyber resilience arsenal, and another 52 percent are planning future investments in this area.[15]

Technologies that provide thorough and automated remediation restore corporate endpoints to their pre-infected, trusted state. For modern cyber resilience, remediation capabilities should also include detection and removal of dynamic and related artifacts. This is essential to prevent malware from re-infecting the network.

Automate orchestration across IT silos

When enterprises automate the orchestration of integrated endpoint security tasks between their complex, distributed security ecosystems and services, they streamline, accelerate, and simplify security processes and operations. Automating low-level tasks and enabling process automation between security controls delivers enterprises cyber resilience that is nimble with faster actions that protect and respond to attacks as they occur. It also provides the organization with better use of limited resources and improved management with coordinated workflow actions.

Integration opportunities across the IT security stack are numerous. With the importance of corporate endpoints to business continuity and their position at the front of the enterprise attack surface, companies should prioritize automated orchestration for endpoint security and management functions.

Orchestration tools that deliver endpoint visibility and the means to coordinate, inform, and execute protection and remediation efforts will greatly enhance a company's security posture and cyber resiliency. Likewise, organizations should adopt cloud-based management of endpoints that provide visibility with remediation maps. This ensures CISOs can coordinate response efforts and track progress when a successful incident occurs.

Reaping the benefits of cyber resilience

> The benefits gained from automation are far-reaching. Companies investing in automation functions experience a strong position of cyber resilience. For instance, 71 percent of security professionals state that automation reduces response time for detection, response, and remediation. Reduced response times, in turn, lead to sizable savings: companies that contain a breach in less than 30 days save US$1 million compared to those requiring more than 30 days.[17]

In addition, reducing response time stops dangerous infections from taking down thousands of endpoints. This is critical in today's world of NSA-powered exploits, such as EternalBlue and EternalRomance, that are used to spread threats laterally through networks like wildfire.

Cyber resilient companies have taken steps to understand the prioritized value of their data and implement their cyber resilience plan and technology. When CISOs do so, they can confidently report to board members that the organization has the strongest risk mitigation plan with thorough resiliency measures that preserve operations, maintain revenue growth, and protect customers' data and the company's reputation in the event of an attack.

Ultimately, automation creates a more efficient SOC that allows analysts to focus their time supporting the company's revenue-generating initiatives that require more thought and expertise (e.g., level three and four analyst functions). The majority of SOC teams (54 percent) claim that automation allows them to better prioritize security operations activities.[18]

This approach relieves the time-consuming re-imaging efforts and "putting out fires" strain on resources—whether due to budget constraints or fallout from the skills shortage—and turns the SOC into a revenue-enabler that helps the business grow.

Conclusion

> Digital transformation has made it possible for companies to take advantage of data that optimize operations, accelerate growth, and increase customer retention. At the same time, cybersecurity has become a necessity to protect the company's valuable data and preserve business operations.

Since then, CISOs have been managing the tightrope balance between risk mitigation and budget and resource constraints. Across people, processes, and technology, optimal cybersecurity requires a level of investment that many businesses either weren't willing to make or didn't feel the pressing need—until a lack of cyber resilience impacted their bottom line.

Ultimately, companies require mechanisms to automate their cyber resilience so it can perform at the same speed and scale as cyberattacks themselves. With market trends driving corporate endpoints forward as the network edge, CISOs should take steps to embrace endpoint resilience.

Ultimately, cyber resilience ensures companies keep running and transforms SOC teams into agents for business growth. By holding operations in check, protecting valuable data, and giving endpoints the automated tools to fend off attacks, corporate cyber resilience ensures companies continue to draw in new customers while retaining highly satisfied customers and growing brand value.

[1] Ponemon Institute. 2018 Cost of Data Breach Study. July 2018.
[2] Capgemini. Big & Fast Data: The Rise of the Insight-Driven Business.
[3] CSO Online. What information in businesses do cybercriminals value?. November 2018.
[4] Malwarebytes. Cybersecurity Resiliency Survey. 2019.
[5] Ibid.
[6] Wikipedia. Ashley Madison data breach. April 2019.
[7] Ponemon Institute. Cost of a Data Breach Study 2018.
[8] Malwarebytes. Cybersecurity Resiliency Survey. 2019.
[9] Ponemon Institute. The Third Annual Study on the Cyber Resilient Organization. 2018.
[10] Ibid.
[11] SANS. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey. August 2018.
[12] Ponemon Institute. Cost of a Data Breach Study 2018.
[13] Ponemon Institute. 2018 Cost of Data Breach Study. July 2018.
[14] Malwarebytes. Cybersecurity Resiliency Survey. 2019.
[15] Ibid.
[16] SANS Institute. 2019 SANS Automation & Integration Survey. March 2019.
[17] Ponemon Institute. 2018 Cost of Data Breach Study. July 2018.
[18] Ibid.