WHITE PAPER:
THE CYBER-RESILIENT ENTERPRISE

# The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence

## Who should read this paper

IT leadership

Symantec

**Content**

## Executive Summary

This paper explains to IT leadership the importance of cyber resilience in the face of evolving cyber crime tactics. It defines the state of cyber resilience and the importance of security intelligence in achieving it. Finally, it paints a picture of the future of security.

## Introduction: From Reaction to Prediction

An important shift has occurred in the security landscape of late. Thanks to rapid business digitization, evolving IT infrastructures, and cyber criminals increasingly adept at exploiting the complexity in today's Internet-enabled world, cyber crime is now top of mind for both enterprises and governments, moving up on a list of concerns from 13th place in 2012 to third in 2014.[1]

The reasons for this are varied. To keep pace in an ever more competitive world, businesses are adopting new ways of doing business, making them more dependent than ever on connected services and exposing them to new security challenges. In addition, the explosion in data leaves organizations vulnerable to attack, while the dearth of properly trained security experts leaves them short-handed. Finally, un-integrated security architecture and poor visibility across tools and processes provide ample opportunity for cyber criminals to exploit vulnerabilities and security holes.

Highly targeted attacks have become the new norm. 2013 became the year of the mega breach due to a 62 percent increase in breaches over 2012, totaling 253 breaches with eight of those breaches exposing more than 10 million identities each[2]. Organizations today regardless of size are struggling to develop a comprehensive security strategy to stop them. A paradigm shift is required—a call to recreate the very idea of security and to change the stance from reaction to prediction. Cyber resilience—an approach that goes beyond specific security solutions to address the growing risks we face as individuals, businesses, and governments—can help us get there. And security intelligence, in all its forms, is the key to cyber resilience—security intelligence that provides the visibility and agile protection today's leaders need to make fast and effective decisions for their organizations.

## A Perfect Storm

A number of factors are combining to make cyber security a top priority for both businesses and governments. Enterprises are increasingly reliant on Internet-connected services to do business, and entire economies can now be damaged by cyber crime. Worldwide, Internet-related economic activity will be worth $4.2 trillion by 2016[3]. The United Kingdom leads the pack, with eight percent of the country's gross domestic product (GDP) currently dependent on online or web-connected services—a number slated to increase to 26 percent by 2016[4].

As a result, governments are also sharpening their focus on cyber crime. In the past couple of years, almost all European Union nations have implemented cyber security programs with the intent to protect citizens, reduce Internet crime, safeguard the economy, and reassure national investors. In the US, President Obama publicly acknowledged that cyber threats pose one of the gravest national security dangers that the country faces[5], a point reinforced in a new Defense News poll that found that nearly half of national security leaders believe cyber warfare is a bigger threat to the US than terrorism[6]. Hence, large investments and a number of directives—including the NIST Cyber Security Framework enacted in February of 2014—are reinforcing cyber security.

At the same time, new IT capabilities and trends such as cloud, mobility, virtualization, and the Internet of Things are increasing complexity and creating gaps. Five years ago, static data centers, and IT teams organized in silos, each focused on securing a different element of the

1- Lloyds Risk Index, 2013
2- Symantec Internet Security Threat Report 2014
3- Ibid. http://www.information-age.com/technology/mobile-and-networking/2093663/uk-has-worlds-most-internet-dependent-economy#sthash.bGh9Kr5W.dpuf
4- Boston Consulting Group (BSG)
5- http://www.informationweek.com/government/cybersecurity/why-businesses-cant-ignore-us-cybersecurity-framework/d/d-id/1113838
6- http://www.defensenews.com/article/20140105/DEFREG02/301050011

infrastructure such as the network, applications, and storage environments were the norm. Now, in addition to managing traditional risks such as targeted malware, data loss, audit scope creep, security updates, and secure authentication and access, IT must contend with a host of thorny new areas and issues related to these emerging trends, not the least of which is the need to tear down the silos and take a more integrated approach to security.

Add to this the problem of data growth. Already massive, and doubling every year, the amount and rate of data growth strains the infrastructure in every conceivable way. The explosion of distributed information has become an attractive target for cyber criminals who take advantage of a patchwork defense strategy to exploit existing gaps, aiming attacks across many vectors simultaneously and involving multiple security controls. If these control points cannot share their attack knowledge, the attack will likely go unnoticed for too long.

## Today's Attacks: Elusive and Targeted

Managing security and keeping up with the latest attack trends is expensive, cumbersome, and far from foolproof. Many targeted attacks go undiscovered for far too long. According to one recent report, 66 percent of breaches took months or even years to discover. And a recent Ponemon Institute report found that, on average, it takes companies three months to discover a malicious breach and more than four to resolve it[7].

Threats are constantly evolving, and cyber criminals' motivations have changed dramatically in recent years. What used to be considered a hobby or a rite of passage has become a sophisticated commercial undertaking which, when successful, can result in significant financial and other rewards. Today's adversaries are sometimes competitors' employees or one's own disgruntled employees trying to gain access to intellectual property or dollars. In other cases, they are funded and supported by countries, mafia organizations, or terrorists.

As a result, attacks are growing more sophisticated. Professional hacker-for-hire operations now exist, composed of members who possess the technical prowess, agility, resourcefulness, and patience necessary to wage relentless campaigns against multiple concurrent targets over a sustained period of time. As the pioneers of the "watering hole" technique used to ambush targets, they possess early access to zero-day vulnerabilities and lie ready and waiting to compromise a supply chain to get at the true target.

These criminals are singling out web-based and mobile platforms and applications. Some focus on very large companies. Others select organizations that lack the levels of security found in larger enterprises. In fact, smaller companies are more exposed than ever: 30 percent of spear-phishing attacks now affect organizations with fewer than 250 employees[8]. The numbers are sobering. Criminals claim 378 million victims per year, adding up, conservatively, to $113 billion in losses annually[9]. Monthly ransomware (a variant of malware) activity increased by 500 percent from 100,000 in January to 600,000 in December, increasing to six times its previous level[10]. Crucially, of the websites serving up malware, 62 percent were from legitimate sites that had been compromised[11].

It's an uphill battle. Unfortunately, attackers have the blueprints to our defenses at their fingertips. They can buy attack toolkits to use against businesses; they are capable of changing their campaigns as needed; and they have the persistence and patience to execute their plans over months and years. In fact, only the most knowledgeable of security experts have the level of expertise that exists in the underground world.

7- Information Week, http://www.darkreading.com/attacks-breaches/why-are-we-so-slow-to-detect-data-breaches/d/d-id/1139970?
8- Symantec ISTR 2014
9- 2013 Norton Report
10- Symantec ISTR 2014
11- Verizon DBIR 2013

## Current Security Strategies Aren't Working

Best of breed solutions *do* identify and block many attacks, which is why it remains a best practice to deploy endpoint security, database monitoring, email and web filtering, and firewalls. However, deploying them on an as needed basis leaves IT with a patchwork of products from a variety of vendors as well as a plethora of procedures and security polices to navigate. The result is greater expense to maintain the products, additional staff to support products with little interoperability, additional training for personnel, a greater number of vendor relationships to maintain, and an overall less effective IT department that's held hostage by its own security solutions, policies, and processes.

Finally, and perhaps worst of all—a fundamental lack of integration results in gaps that allow attackers through. In fact, the average number of total incidents detected by IDP/IPS solutions is an unimpressive 32 percent[12], and the majority of breaches take months or more to discover[13]. Organizations that have multiple layers of security products think they may be covered based on the high number of logs and alerts they receive, but in reality, it's a lot of noise to sift through. In many cases, they may not be effectively prioritizing and responding to the most urgent threats. This means the enterprise could be a lot more effective and resilient when it comes to security.

To make matters worse, security staffing and skills shortages are widespread. Only 17 percent of large organizations believe they have the right level of security skills in house to adequately address malware detection, response, and analysis requirements in all cases[14]. Even worse, a mere 12 percent of enterprises have an appropriate number of employees in their IT security organizations to adequately address malware detection, response, and analysis requirements in all cases[15]. This presents an ominous scenario: many enterprises are under-skilled and under-staffed as the malware landscape grows more dangerous.

## The Solution: Cyber Resilience

Clearly, organizations must rethink their approach to security. Enterprises and their users will never be completely free from cyber risk, however they can become cyber resilient. A strategic partnership between the security team, IT team, and business leaders must be established so that security and technology are enabling rather than hindering business. A balance creates understanding and protection against the inescapable cyber risks of today while supporting the business.

Cyber resilience does not promise immunity from cyber attacks nor does it purport to eliminate risk. Eliminating all cyber risk is impossible, and in fact would impede agility, for an environment with an acceptable level of risk enables innovation. To achieve cyber resilience, organizations must move away from a fragmented security infrastructure toward one that is enterprise-wide, integrated, shares threat intelligence, and leverages security services.

Organizations can begin by harnessing the internal intelligence that is collected by their security technologies and correlating it with global threat intelligence, developing more security conscious employees, and utilizing security services to sift through the noise and prioritize threats. Organizations often find themselves in reactive mode, putting out fires and assessing damage after the fact. What they should be doing is making the time to think proactively and establish a more robust and resilient security strategy to better prepare for, protect, detect, and respond to emerging threats.

12- 2012, Symantec MSS Install Base Survey
13- Verizon 2013 Data Breach Investigations Report
14- ESG Research Report: Advanced Malware Detection and Protection Trends
15- ESG Research Report: Advanced Malware Detection and Protection Trends

## Security Intelligence: the Key to Cyber Resilience

Without complete visibility into the environment and the current threat landscape, it's easy to be blindsided by an attacker. To achieve cyber resilience, enterprises need security intelligence. What is meant by security intelligence? Intelligence cuts across various security functions such as internally collected data feeds, global threat data, and security personnel expertise to create a holistic approach that pulls the security pieces together. It's difficult to manually sift through alerts, stay on top of vulnerabilities, consistently apply security policies across various systems and endpoints, and assess what is happening in the market without a cyber resilient security strategy. Security intelligence enables better business decision-making, better organizational processes, increased protection from cyber attacks, and better preparation when they do occur—resulting in a business that is more resilient and agile. What's required is a multi-layered security approach that encompasses people, processes, and technology.

*People*

Security intelligence in the form of data is critical, but big data analytics won't solve the problem by itself. Enterprise leadership must think beyond the devices and data to the people at the organization, specifically how to develop their security intelligence. Security analysts assessing and analyzing the data must understand what the technology has revealed, how to recognize a potential compromise or incident, and then apply the art and science necessary in the final step to determine whether the incident is truly a security threat and how to respond. Many organizations are not properly staffed to adequately assess and prioritize threats and must leverage an outside vendor who can provided managed security services for them.

Educating employees on security policies and best practices, especially as it relates to data loss and mobile devices, is also crucial. A surprising amount of data loss occurs not through the malicious actions of attackers, but through the actions of well-meaning employees who unknowingly put company data at risk. For example, employees frequently transfer corporate data to unauthorized cloud applications, where the security, in most cases, depends solely on the outside vendor. In fact, a recent survey found that seven out of 10 organizations are running cloud applications not officially sanctioned by their IT departments[16]. According to a survey by the Ponemon Institute, 50 percent of employees who change companies take documents, applications, or data that they've developed and don't see it as wrong[17]. This means precious intelligence is falling into the hands of competitors, causing damage to the losing company and adding risk to the unwitting receiving company.

In fact, employees are moving intellectual property outside the company in all directions. Over half admit to emailing business documents from their workplace to their personal email accounts, and 41 percent say they do it at least once a week. Forty-one percent also say they download intellectual property to their personally-owned tablets or smartphones. Once corporate data is on the personal mobile device, it is not well protected. Nearly one in two people fail to take basic precautions such as using passwords, having security software, or backing up files[18]. These activities expose potentially sensitive data to greater risk of compromise than leaving it on the company-owned device, and the risk increases because the files are generally not removed when they are no long needed.

Enterprises must develop enforceable workplace and mobile security policies that provide the dos and don'ts of information use in the workplace and when working remotely, including intellectual property theft awareness training. It should be clearly spelled out what employees can and cannot take with them when they leave the company. The risks of posting certain information to social sites must be reinforced. Social engineering and trawling social sites are becoming the best ways cybercriminals have for gathering information for

16- 2013 State of Cloud Application Access Survey, Identity Management Firm, OneLogin
17- What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk, Symantec Corporation and Ponemon Institute
18- The Norton Report 2013

targeted attacks or to gain access to corporate or personal devices.  Finally, employees should be educated about how to use their privacy and permission settings and the risks of downloading rogue applications.

*Process*

The road to cyber resiliency is not a single step process, but one that requires continual refinement as threats change and organizational needs evolve. To facilitate this process, it's helpful to think about building cyber resilience in five areas: Prepare/Identify, Protect, Detect, Respond, and Recover. Using current tools (frameworks or standards), enterprises can analyze their own cyber security strategy to determine how it measures up. The first step may be a risk assessment to determine the vulnerabilities that exist in their security posture, or procedural changes to better respond to incidents when they are detected. It's important to realize that it's not the steps that should be the focus but the results, since every organization has unique systems and different security needs. Whatever the process, the end result should be an improved ability to make informed business decisions that positively impact the security of the enterprise and the development of a well thought-out security strategy that utilizes all the available security intelligence and is agile enough to respond to a constantly changing threat landscape.

*Technology*

Network security alone isn't going to solve the problem because attacks arrive across email, gateway, and endpoints. Security intelligence must correlate and sift through all of the threat data collected across these various security control points. This is where big data analytics come into play. A great deal of data is needed to see patterns that might indicate incursion versus discovery versus capture. A big data analytics capability can connect the dots and see the data from different angles. However, the unwieldy nature of big data means that security efforts must now be predictive rather than historic. To protect the information you manage and integrate intelligence into your policy framework, you must ensure that all systems are using consistent, reliable intelligence gathered and monitored for abnormalities.

Initially, security intelligence increases cyber awareness, preparing the organization for the possibility of an attack. Once you've secured access via access control and identity management tools, you're able to protect and govern data from cyber threats no matter where the data lives. By harnessing security intelligence, the cyber resilient organization creates a proactive IT department with visibility across the entire environment, one with deep, data-level integrations that yield insight, and that constantly evolve and respond as attackers become more advanced. By correlating security intelligence, IT can quickly detect and remediate a potential issue before it spreads, resulting in reduced damage and cost. Additionally, maintaining an environment free of infection protects customers and partners. Such an organization is an unappealing target for a cyber criminal.

## The Future of Security

In an ideal future, enterprises need not manage their security at all. It would be managed and integrated for them by a security provider able to leverage great economies of scale to reduce costs and raise protection capabilities. Imagine a large, complex, cloud-based, multi-tenant repository that holds months or years of security data from many organizations—a repository that can be mined using big data techniques to identify attacks that don't span hours, but weeks, months, or years. The advantage of this big data approach is that companies could spend less time being reactive and more time achieving strategic objectives.

Eventually, data can be collected not just from your computer, but also from hundreds of thousand of companies, leveraging a massive global network, where each company submitted just the data they chose. This vast repository of data could be leveraged to uncover new, targeted attacks that would otherwise be invisible. You wouldn't be left to your own devices to protect the enterprise. Rather, you'd be part of a

community that shared wisdom to collectively better defend its networks. As a result, even the most highly complex and targeted attacks could be discovered within minutes or hours rather than extended periods of time, as is too often the case now.

A managed service is a start to delivering on this vision. Managed security offerings can range from security monitoring and prioritization to advanced threat protection and incident response management, all to build a resilient security strategy that allows you to quickly prepare, protect, detect, and respond to complex cyber attacks.

## Conclusion: Looking Ahead

You don't need another security product. You need a cyber resilience strategy that extends across your people, technology, and processes. Imagine a new, service-based approach that offers a single unified perspective of all of your systems—on-premise systems, cloud systems, mobile devices, traditional endpoints, and networks. Cyber resilience increases overall business confidence and capability. When employees are trained and aware of security polices, and when the intelligence that is gathered is used to shape processes and impact business decisions, enterprises are better prepared for threats. An organization that collects, consolidates, and correlates security intelligence across control points with global threat intelligence gathered across companies, industries, and geographies is better able to detect attacks in real-time, quickly respond, and prepare for future threats. Security intelligence, in all forms, is critical for today's organizations to stay agile and resilient.

**Contact your Symantec account representative or reseller partner today to discuss how you can start building cyber resilience into your security strategy.**

Get more information about cyber resilience and stay informed at the Symantec cyber resilience microsite. go.symantec.com/cyber-resilience

**About Symantec**

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com