

CYBER-RESILIENCE:

THE KEY TO  
BUSINESS  
SECURITY

#PASS2018

<b>Introduction and summary</b>	<b>3</b>
<b>The evolution of cyberthreats</b>	<b>5</b>
<b>Challenges for organizations to become cyber-resilient</b>	<b>7</b>
<b>Adoption of cyber-resilience</b>	<b>13</b>
<b>Characteristics of cyber-resilient companies</b>	<b>18</b>
<b>Conclusions</b>	<b>22</b>

## Introduction and summary

A quick Google search of the term “resilient companies” turns up 44,400,000 results in less than a second. This concept, defined as “the capacity to recover quickly from difficulties and come out stronger”, has become key to businesses that face a large number of risks born from the context of a global economy: from cyberattacks to large-scale, global fraud and theft of personal data, to the potential adverse effects of technological advances such as artificial intelligence, geoengineering, and synthetic biology that can affect the environment, the economy, and ultimately human beings themselves.

We are witnessing a transformation of social relations, the business fabric, and government efforts; a transformation that bases its potential on technology, data, and artificial intelligence that collects, filters, classifies and correlates large-scale data in order to learn from it and make predictions.

Thus, the digital transformation affects daily life and the functioning of organizations in such magnitude that, nowadays, it has become a company’s source of wealth and provides a competitive edge to countries. Appropriating this wealth is no longer a matter of armed wars, but of a “simple” digital transfer of that wealth, of the data assets that identify and differentiate the country in question. All it takes is a cyber-battle to attack key computers and obtain the information necessary to overthrow a government or to take away its competitive advantage.

Being resilient is an imperative, understanding the term “resilience” as “the inherent capacity of an organism, entity, company or state that allows it to face a crisis without its activity being affected”. It is not just a matter of recovery, but also of resurgence and empowerment after an unfavorable turn of events.

In the context of security, cyber-resilience refers to the ability of an organization to maintain its main

goals and integrity against the latent threat of cybersecurity attacks.

A cyber-resilient company is one that can prevent, detect, contain and recover, minimizing exposure to an attack and its impact on business, against countless threats to data, applications, and IT infrastructure. And especially against devices, where the organization’s most valuable assets reside, since reaching them also implies attacking the integrity of identities and users.

As hazards increase, traditional approaches to maintaining cyber-resilience are no longer enough. Many entities survive in a precarious equilibrium, and the slightest alteration, however small in relation to the size of the organization or the importance of its activities, can precipitate a crisis. To avoid collapse, cybersecurity management will need a thorough revision and implementation of new protection models.

Until recently, financial entities and governments were the main targets of cyberattacks. Today, the development of businesses of any size and sector depends to a greater or lesser extent on the Internet and, consequently, the threat has become universal. As these dangers increase, current approaches to maintaining cyber-resilience no longer work. Cybersecurity management is in need of a thorough revision with new and improved security models.

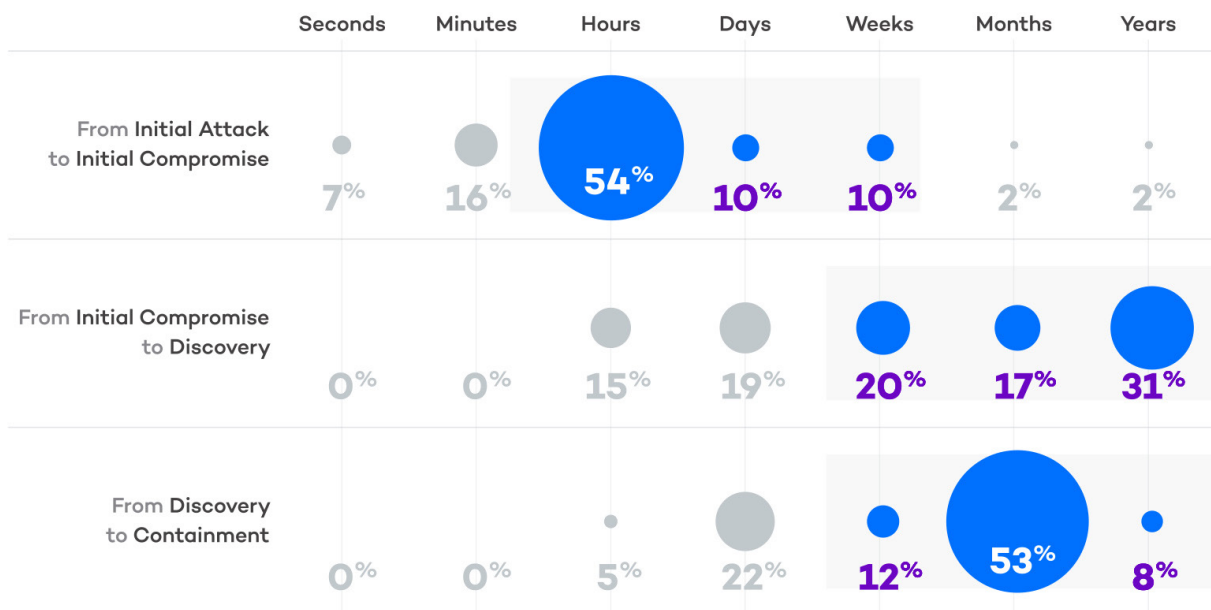
In fact, we have just recently witnessed the Meltdown and Specter cases, which revealed the vulnerabilities not only of software but also of hardware. Similarly, between 2011 and 2014, we saw how energy companies in Canada, Europe, and the United States were attacked by the cyber-espionage group Dragonfly. In May 2017, the WannaCry ransomware held hostage public and private organizations in telecommunications, health, and logistics. Also in 2017, the NotPetya ransomware targeted major European companies in virtually all sectors.

But while the collective consciousness in this area is slowly growing, confusion grows along with it. Organizations and their executives are overwhelmed by the challenge. According to a study conducted earlier this year by Forrester Consulting for Hiscox<sup>1</sup>, through a survey of more than 4,100 executives, CISOs, IT managers, and other key positions in the United Kingdom, EE.UU., Germany, Spain and the Netherlands, 57% of the surveyed organizations claim to be prepared to respond to security attacks. However, a more detailed study through indirect questions shows that 73% of the companies surveyed are at low levels of maturity and are beginners in the field of detection and response to cyberattacks. Only 11% of organizations have experts on their security teams, and thus well prepared to face cybersecurity challenges.

stance: comprehensive, strategic, and persistent, with a new approach to their security program that can protect without imposing undue restrictions on their business. And this new stance must be based on strengthening preventive defenses, assuming that they can be overcome by the attackers or that they are already present in the organization. New techniques for penetrating defenses and hiding malware are allowing threats to remain in corporate networks for long periods without being detected.

Nor can internal threats be forgotten. Personnel attacks with privileged access represent one of the greatest threats to the security of corporate and customer data. Investigations conducted by Ponemon Institute point to hackers and criminal insiders as the main culprits of security holes and data leaks.

To increase and maintain their resilience to cyberattacks, companies must adopt a new



Data from the 2016 DBIR.

<sup>1</sup> 2018 Hiscox Cyber Readiness Report <https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf>

The paradigm shift toward a resilient company consists in avoiding the compromise of company assets and detecting attacks before there is damage with a limited response time. Now is the time for the materialization of tendencies such as Threat Hunting, forensic investigation to identify the root cause of the attack, Endpoint Detection and Response (EDR), and constant endpoint monitoring. It is fundamental to generate forensic data in real time in order to thoroughly investigate incidents.

At the same time, a company that is mature in resilience will admit that failures and errors do occur, and has the means to restore normal operations to secure assets and its own reputation. In short: the organization is able to emerge strengthened from the incident, applying changes that improve its defense situation.

## The evolution of cyberthreats

Cybercrime is an attractive and highly lucrative business. Attackers have more and better resources at their disposal than ever — both technical and economic. This allows them to develop increasingly sophisticated attacks. This results in more complex and more dynamic threats, in addition to a greater number of attacks.

[Equifax](#), CCleaner, WPA2, Vault7, CIA, KRACK, NSA, [the elections hack](#)... these are just a few of the main characters of the business cybersecurity landscape of recent months. They were the protagonists of massive infections, data theft, ransomware attacks, hacked applications used to launch attacks against a country or carry out targeted attacks against specific large companies, or exploit vulnerabilities affecting billions of devices.

The havoc that ensued from three recent events must be taken into consideration. From 2011 to 2014, the Dragonfly cyber-espionage group consistently made headlines, rapidly expanding its activities and jeopardizing the North American and European energy sector. Dragonfly took advantage of two fundamental components of a malicious program, namely remote access tools, gaining access to and controlling infected computers.

In 2017, **there were two attacks that stood out especially for the impact and damage they caused: WannaCry and GoldenEye / NotPetya.**

[WannaCry](#) appeared in May, spreading and wreaking havoc on corporate networks around the world, proving to be one of the largest attacks in history. Although we have seen much more powerful attacks in the past (such as Blaster or SQLSlammer, to name just two), at least in terms of number of victims and rate of spread, the truth is that the damage they caused was merely collateral. However, WannaCry is a ransomware with network worm functionality, so every infected computer ended up with its documents being hijacked.

[Goldeneye / NotPetya](#) was the second attack with the greatest repercussion of the year, as an aftershock of the earthquake that was WannaCry. Despite the fact that its victims were initially limited to a specific geographical area (Ukraine), it ended up affecting companies in more than 60 countries.

The attack, carefully planned, was carried out through a very popular accounting application among companies in Ukraine, M.E.Doc. The attackers compromised the server updates of said software, in such a way that all the computers with M.E.Doc installed could be infected instantly and automatically.

In addition to encrypting the files, if the logged-in user had administrator permissions, the malware went for the MBR (Master Boot Record) of the hard disk. At first it seemed to be a ransomware in the vein of WannaCry, but after analyzing it thoroughly **it became clear that its authors did not intend to let the ransomed data to be recovered.** Days later, the Ukrainian government openly accused Russia of being behind the attack.

And in the field of cybersecurity, 2018 could not have started off worse: [the security flaw](#) found in Intel, AMD and ARM processors was deadly serious. This architectural design failure, accompanied by errors in the operating system, dropped like a bomb in the technology sector, and all worked against the clock to close the gaps as soon as possible.

The flaw, used by the **Meltdown exploit** in Intel architectures, is especially critical from the point of view of sensitive data exfiltration — information such as credentials, emails, photos and other documents — allowing the attacker, through a malicious process that runs at the user level on the computer or server, to read the memory of other processes, including privileged processes of the operating system kernel.

Both domestic users and practically all companies are affected, since Specter acts on computers, laptops, Android phones as well as on-premise servers and Cloud servers. The more critical the information being handled, the greater the risk of being the target of an attack using this tool.

And there are plenty more real cases reaching the giants of different sectors. For example, **Apple**, which was caught in the crossfire of arrests made in China of 22 people who allegedly trafficked with company data. All indicators point to an inside job, since some of the detainees worked for companies subcontracted by Apple and had access to the trafficked data.

**HBO** has also suffered several cyberattacks in recent months. In one of them, servers were compromised by stealing complete episodes not yet premiered from different television series, as well as internal information.

**InterContinental Hotels Group (IHG)** was the victim of customer data theft. Although the company said in February that the attack had only affected a dozen of its hotels, it has now come to light that they had POS (Point of Sale) terminals infected in more than 1,000 of their establishments. Among the different brands of hotels that the group owns are Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels, and Crowne Plaza.

The **Saber Corporation** is a North American company that manages reservations for 100,000

hotels and more than 70 airlines around the world. An attacker obtained the credentials to access one of the company's reservation systems, accessing payment information and reservation details. This system manages reservations for individuals and travel agencies in 35,000 hotels and accommodation establishments. They were compromised from August 10, 2016 to March 9, 2017, a full seven months.

But the biggest security breach of the year — and one of the worst in history — would come a little later, when it was learned that the credit reporting giant, **Equifax**, had been compromised. The company has warned that the total count of affected individuals amounts to 147.9 million. The question is: could such an attack have been prevented? The answer, of course, is yes. **Equifax left the door open to cybercriminals by not updating Apache Struts**, the web application development framework. This unpatched vulnerability allowed hackers to expose the social security numbers, postal addresses, and driving license numbers of millions of people. This is a case in point showing how a failure to comply with basic security measures such as patching software can have colossal consequences.

With real cases like these, it is not surprising that 75% of companies (according to a recent survey by McKinsey<sup>2</sup>) consider that cybersecurity is a priority for their proper functioning. Being prepared for a cyberattack is a major concern in such industries as banking or automotive production, industries in which one would think that they would be worried about other great changes and risks. We're dealing with a universal and horizontal threat.

The threat is too large and the attackers behind it are growing both in number and in sophistication too quickly.

To increase and maintain their resilience to cyberattacks, companies must adopt a new

<sup>2</sup> <https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world>

stance: comprehensive, strategic, and persistent, with a new approach to their security program, which can protect companies without imposing undue limitations on their business.

This new approach should be based on strengthening preventive defenses, but with the assumption that attackers can overcome them and may in fact already be present in the organization, whether as infiltrator or insider. The paradigm shift will be to prevent them from compromising the company's assets by detecting them before the damage is done, and responding as soon as possible. At the same time, a resilient company must be able to emerge stronger from the incident, applying changes that improve its defense situation.

## Challenges for organizations to become cyber-resilient

Every entity, company, organization, or state is subject to tensions derived from events, changes, and incidents that occur in their environment. These situations of stress are new challenges whose resolution will affect the functioning of the organization until the situation can be managed through automation.

When it comes to the security of organizations, the stress situation in question requires a reaction that involves a new focus on the security program throughout the organization. Companies must identify assets with the greatest value and establish a new model of security governance that centralizes, with an expert security team, the supervision of all cybersecurity efforts throughout the company. It is here that the head of this team gains visibility and participates in the decision making of the organization, forming part of the executive team.

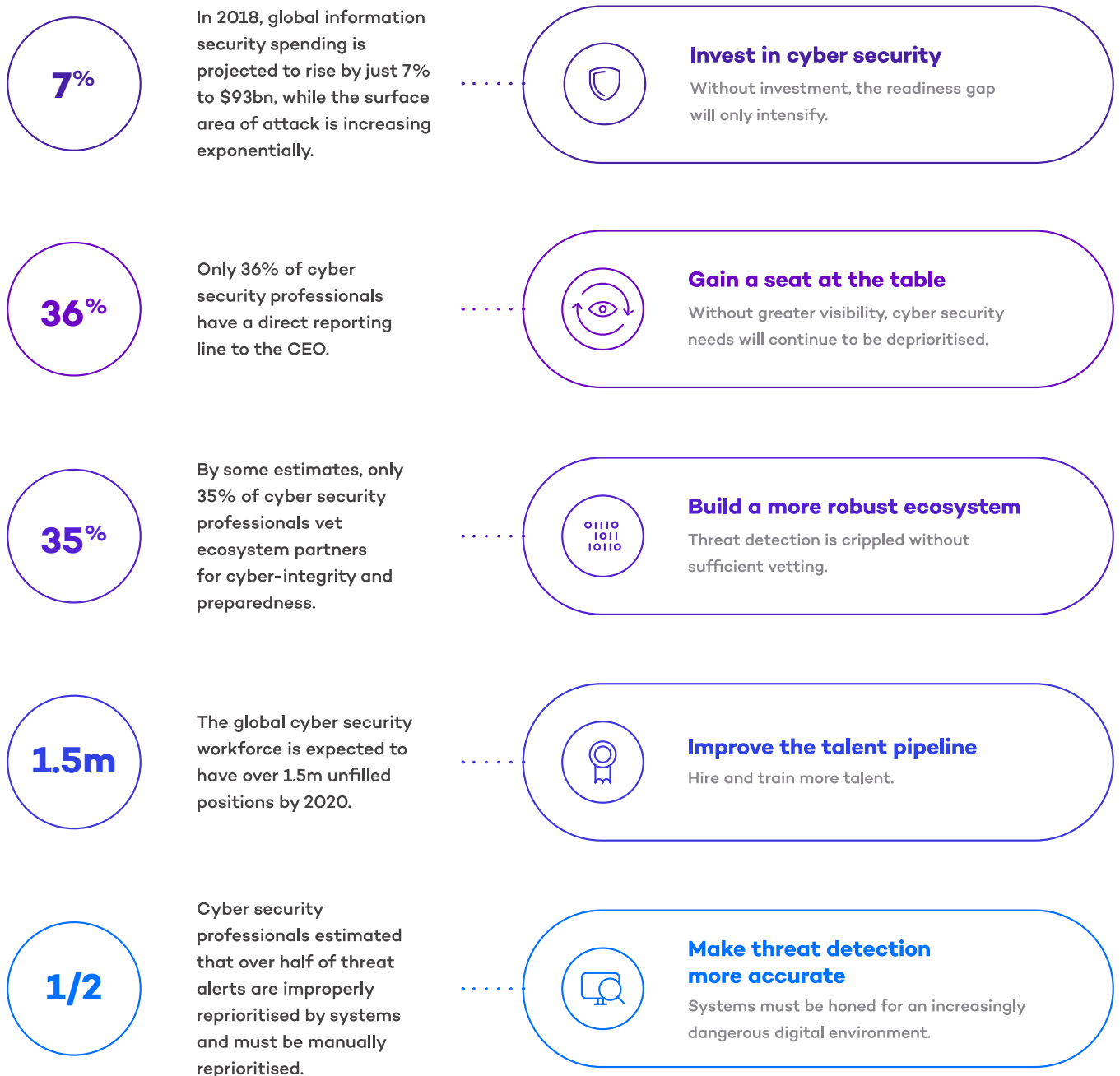
### More Threats, Higher Intensity

In the United States, the Comprehensive National Cybersecurity Initiative (CNCI) was launched with the Bush Administration in January 2008. This initiative introduced a differentiated approach to identifying existing and emerging cybersecurity threats, finding and blocking existing vulnerabilities, and learning from actors trying to gain access to federal information systems. President Obama issued a statement that "cyberthreats are one of the most serious economic and national security challenges we face as a nation" and that "the economic prosperity of the United States in the 21st century will depend on cybersecurity."<sup>3</sup>

<sup>3</sup> [https://www.es.w3eacademy.com/wiki/State\\_security](https://www.es.w3eacademy.com/wiki/State_security)

## Moving towards cyber resilience

The capacity to recover quickly from difficulties and end up stronger.



**Figure 1.** Technological progress is undoubtedly driving the growth of companies. Organizations and the world in general are more connected than ever and the pace of current technological development is the most advanced that has ever existed. This interconnectivity brings both opportunities and risks.



In December of 2017, President Donald Trump's administration published a national strategy document<sup>4</sup> citing cybersecurity issues dozens of times, and did not shy away from naming countries that will be likely to use endpoint networks as a weapon against the US.

This document specifically states that hackers and the governments of Russia, China, North Korea, and Iran have the power to destabilize the economy and threaten the critical infrastructure of the nation, and that the United States will dissuade, defend and, when necessary, defeat Threat Actors who use cyberattacks against it.

It is a reality: all over the world, the threat of cyberattacks is growing both in quantity and intensity and the rapid and unstoppable evolution of digital transformation is helping to create new opportunities for hackers. Here are some figures to illustrate the clear symptoms of this trend:

- Worldwide, more than 100 billion lines of code are created annually, generating millions of vulnerabilities in computers and servers.
  - Many companies report thousands of attacks each month, ranging from the trivial to the extremely serious.
  - Several billion data sets are violated annually.
  - In 2017, hackers produced around 120 million new variants of malware. To date, the total number of malicious software registered by AV-TEST is close to 800 million<sup>9</sup>.
- 10 million new devices connect to our world every day. It is estimated that by 2020, interconnected devices will be at 20.8 billion<sup>5</sup>.
  - Organizations are investing up to \$ 500 million in cybersecurity<sup>6</sup>, and yet 50% of CEOs at companies with profits of over \$500 million do not feel prepared to face cyberattacks with any guarantees<sup>7</sup>, and 82% of managers are concerned or very concerned about cybersecurity<sup>8</sup>.

<sup>4</sup> <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>

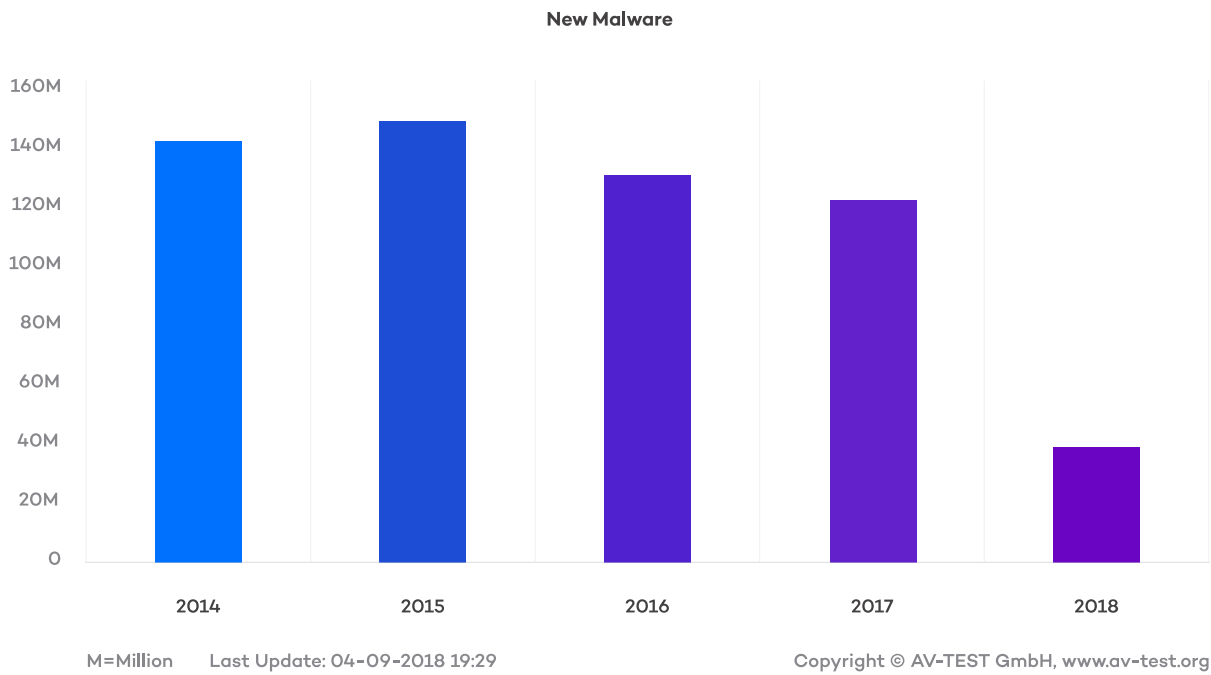
<sup>5</sup> [https://www.isaca.org/chapters7/Monterrey/Events/Documents/20172408\\_Ciberseguridad\\_Fundamental\\_Trans\\_Digital.pdf](https://www.isaca.org/chapters7/Monterrey/Events/Documents/20172408_Ciberseguridad_Fundamental_Trans_Digital.pdf)

<sup>6</sup> <https://cybersecurityventures.com/cybersecurity-market-report/>

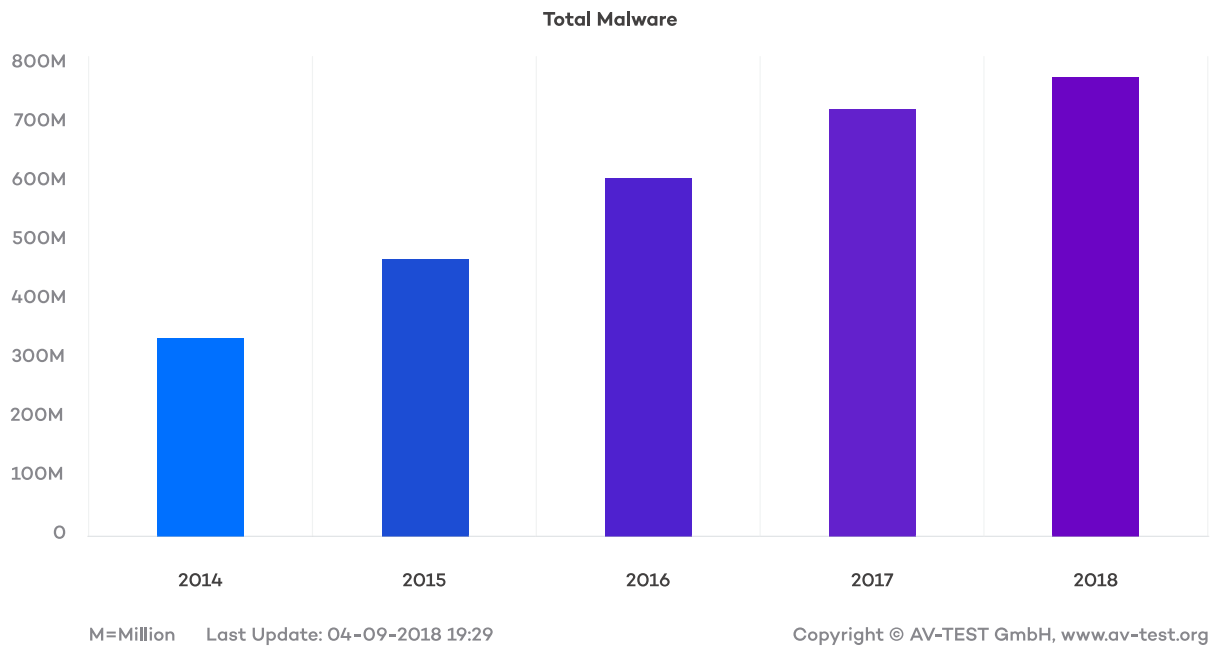
<sup>7</sup> Global CEO Outlook 2015 – KPMG. <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/08/global-ceo-outlook-2015.pdf>

<sup>8</sup> ISACA/RSA Conference State of Cybersecurity study

<sup>9</sup> <https://www.av-test.org/en/statistics/malware/>



J.P. Morgan Chase & Co. doubled its annual cybersecurity budget from \$250 million to \$500 million in 2017. Bank of America declared an unlimited budget when it comes to combating cybercrime.



<https://www.av-test.org/en/statistics/malware/>. Updated on April 9, 2018.

Paradoxically, most companies that were victims of NotPetya and WannaCry probably would have said they were well protected at the time of the attacks. Even when a company is not a primary target, it runs the risk of being damaged by malware in attacks against widely used software. And despite all the new defense systems, companies still need about 191 days on average to detect a covert attack, improving somewhat on the 201 days that organizations took to detect the gap in 2016<sup>10</sup>. The damage that an attacker can inflict in that timeframe should not be underestimated.

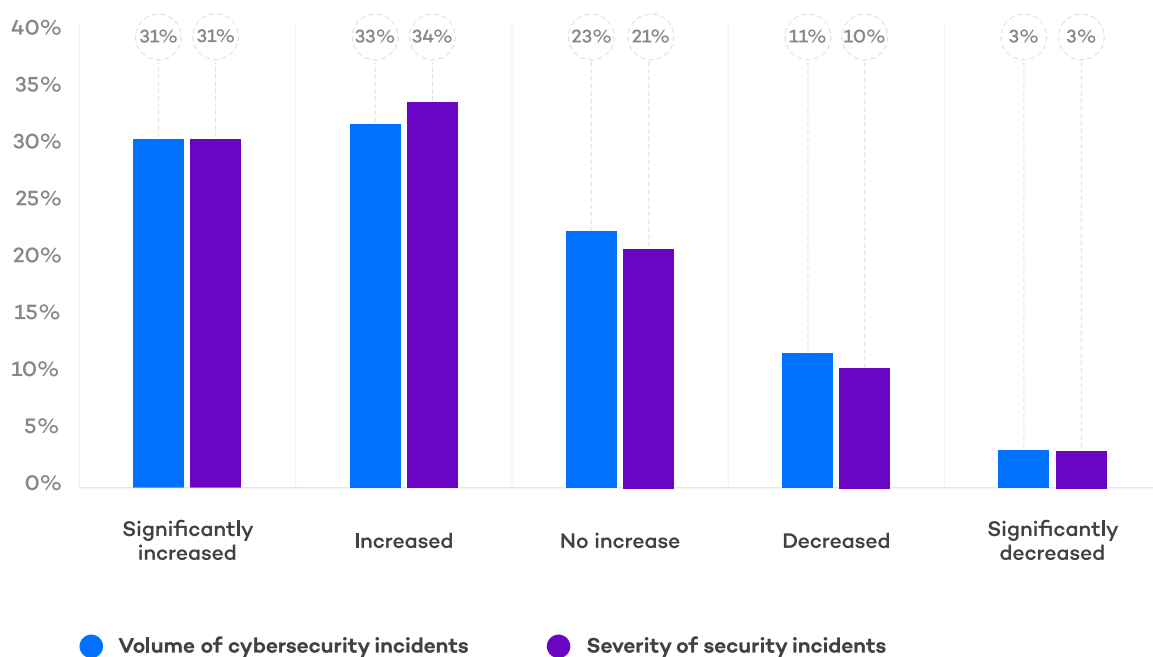
The 2016 SANS Institute Survey on Incident Response<sup>11</sup> revealed that 21% of organizations had a MTTD (Mean Time to Detect) of two to seven days, and only 29% could detect an incident in 24 hours or less. The same study indicates that only

18% of organizations could move from detection to response (MTTR) in a day or less. Worse still, 38% of the survey admitted that, in general, they do not respond in less than a week.

According to the study on the importance of resilience to strengthen the security situation in companies, conducted by the Ponemon Institute and published in March 2018, the severity and volume of security incidents that companies are experiencing increases concordantly with the time needed to resolve them.

As shown in Figure 1, taken from the Ponemon Institute's study of cyber-resilience, 64% of the companies surveyed indicate that the volume has increased and 65% of them indicate that the severity has increased.

**Figure 13. How has the volume and severity of security incidents changed in the past 12 months?**



**Figure 1.** Evolution of the volume and severity of security incidents in the last 12 months according to the Ponemon Institute study from March 2018

<sup>10</sup> 2017 Cost of Data Breach Study (Ponemon Institute for IBM Security)

<sup>11</sup> <https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047>

The increase in volume and severity has a negative effect on the time of detection and response, which has increased significantly. In Figure 2, it is shown that 57% of the companies surveyed say that time has increased.

rapid pace of cyber risk evolution<sup>12</sup>, in many cases with an erroneous approach and an inefficient stance. Some widespread malpractices include:

- Delegating the problem to the IT department.** Many executives treat cybersecurity as a technical problem and delegate it to the IT department. This reaction, which is partly due to the many technical problems that cybersecurity presents, does not take into account that defending a business is different from protecting servers. Defending a business requires a sense of what's at stake, according to business priorities; the business model and the value chain; and the risk culture, roles, responsibilities and governance of the company.

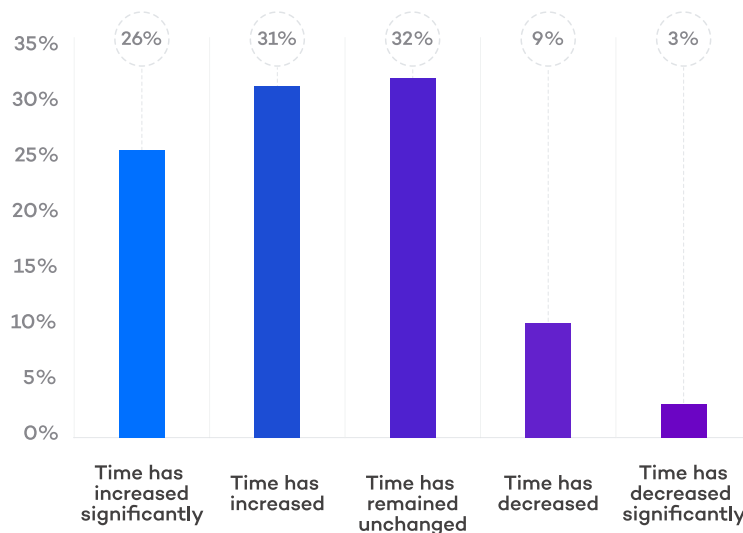
**Complexity of IT infrastructure**

Growing complexity is making companies more vulnerable. While cybercriminals perfect their skills, companies become increasingly digital, opening new doors to vulnerabilities and cyberattacks. Assets that range from new product designs to distribution networks and customer data are now at risk. Digital connectivity is also becoming increasingly complex, using a simple digital connection to unite thousands of people, innumerable applications and servers, workstations, and other devices. An organization's assets are now more exposed than ever before.

**Some Common Mistakes**

Corporate cybersecurity struggles to maintain the

**Figure 14. In the past 12 months, how has the time to detect, contain and respond to a cyber crime changed?**



**Figure 2.** Evolution of the average time of detection and response to security incidents in the last 12 months according to the Ponemon Institute study from March 2018

<sup>12</sup> The AV-TEST Institute registers more than 250,000 new malicious programs every day. <https://www.av-test.org/en/statistics/malware/>

- The **IT department** alone can not address cybersecurity, which should be treated as a corporate issue.
- **Following the trend of using high-profile “hackers” or expert resources to solve the problem.** Other companies assume that the threat will disappear if they hire enough high profile “hackers”. But even the best professionals do not have the ability to anticipate and defend against all attacks against devices in a complex network. The solution requires experts, yes, but also technologies and processes that are geared up and trained for the job. This implies investment in the mid-term and must be sustainable over time to build awareness and involvement of all the company departments, in the risk and its implications, including management.
- **Treating risk as a problem of compliance with the applicable regulations.** Some companies apparently introduce new security protocols and verification checklists every two days. But these efforts often provoke an undue focus on formal compliance, rather than real resilience.
- Knowing and implementing the best defenses against current and potential threats.
- Being prepared for a moment when adversaries can bypass all security technologies and detecting them, containing them and remedying their actions as soon as possible to minimize corporate damage.
- Adopting a crisis position which continuously and actively seeks threats, and detecting vulnerable points that can later be used by threat actors to reduce the attack surface.
- Managing at the corporate level any communication of a breach.
- Defining and constantly executing initiatives to minimize risk and reinitiate the cycle of continuous improvement in the management of corporate security.

**Adaptation is essential.** The organization’s processes, technologies, tools and security services should be reviewed and adjusted as threats evolve in a process of continuous improvement based on wariness. Being resilient implies that this adaptation has to be carried out in the minimum time interval, at the maximum speed, even in real time.

## Adoption of Cyber-resilience

With this complex and real panorama in mind, how can companies intending to protect their assets in the most efficient way possible achieve this more adaptive, complex and collaborative approach in their struggle?

**Cybersecurity should be treated as a problem of corporate risk management,** not as a problem embedded in IT. The key elements of its management include:

- Prioritizing the most valuable assets of the organization.
- Prioritizing, knowing and understanding the most relevant adversaries and threats for each organization.

## The complete approach to cybersecurity management in companies

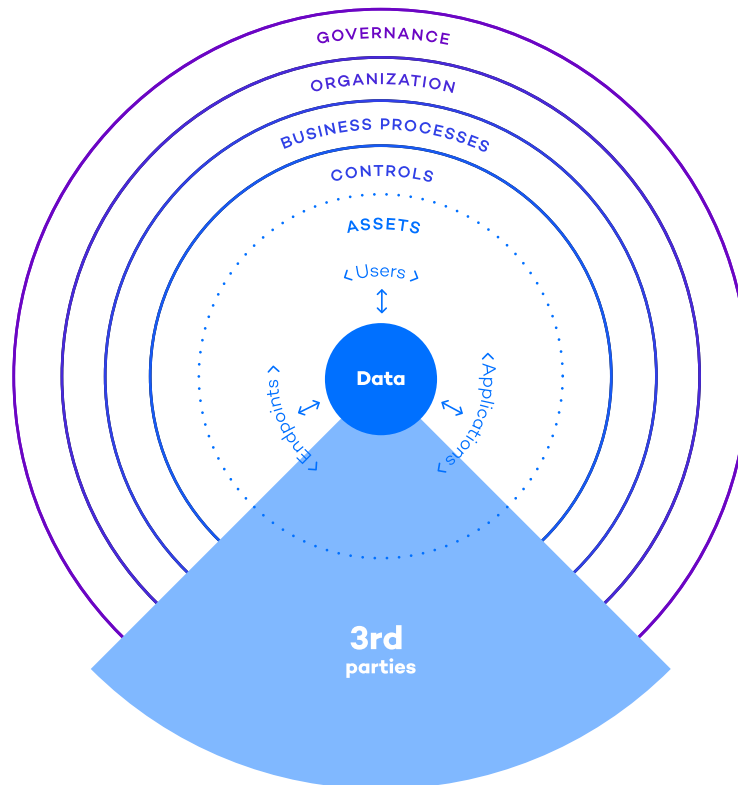


Figura 4. The complete approach to cybersecurity management in companies.

**Companies must seek out and mitigate their risk at all levels.** Creating a complete record of all assets, from data to applications, and monitoring all actions that are carried out with them is a process that is long and tedious, but necessary. Companies must take advantage of the tools and services that automate these tasks of profiling, cataloging, and monitoring their assets (humans, data, infrastructure) for prevention and/or early detection of adversaries.

### Establishing a “resilience cycle”.

Organizations need to understand and adopt the “resilience cycle” process, which will help security teams to continually build on the experience of blocked and/or detected threats.

This requires that they learn and adapt to the key phases of resilience:

- **In the pre-incident phase**, through the ability to better prevent and resist threats, including advanced technologies that detect known and unknown or zero-day malware.
- **During its execution**, by reacting quickly with detection, containment and response to sudden events that threaten the organization to minimize its impact on business; taking advantage of the new paradigms that arise as a result of the monitoring and visibility capabilities that Endpoint Detection and Response (EDR) solutions provide.





Assets	Threats	Controls
 <b>Data</b>	<ul style="list-style-type: none"> <li>• Data breach</li> <li>• Misuse or manipulation of information</li> <li>• Corruption of data</li> </ul>	<ul style="list-style-type: none"> <li>• Data protection (eg, encryption)</li> <li>• Data-recovery capability</li> <li>• Boundary defense</li> </ul>
 <b>People</b>	<ul style="list-style-type: none"> <li>• Identity theft</li> <li>• “Man in the middle”</li> <li>• Social engineering</li> <li>• Abuse of authorization</li> </ul>	<ul style="list-style-type: none"> <li>• Controlled access</li> <li>• Account monitoring</li> <li>• Security skills and training</li> <li>• Background screening</li> <li>• Awareness and social control</li> </ul>
 <b>Endpoints</b>	<ul style="list-style-type: none"> <li>• Malware</li> </ul>	<ul style="list-style-type: none"> <li>• Control of privileged access</li> <li>• Monitoring processes</li> <li>• Malware execution prevention</li> <li>• Network controls (configuration, ports)</li> <li>• Inventory</li> <li>• Secure configuration</li> <li>• Continuous vulnerability assessment</li> </ul>
 <b>Applications</b>	<ul style="list-style-type: none"> <li>• Manipulation of software</li> <li>• Unauthorized installation of software</li> <li>• Misuse of information system</li> <li>• Denial of service</li> </ul>	<ul style="list-style-type: none"> <li>• Email, web-browser protections</li> <li>• Application-software security</li> <li>• Inventory</li> <li>• Secure configuration</li> <li>• Continuous vulnerability assessment</li> </ul>

Figure 5. Risks and controls to be implemented at all levels, from data and entities to endpoints and the applications that run on them.

- **In the post-incident phase**, by absorbing impacts while continuing to achieve strategic security objectives and reconstructing the operating environment in such a way that future sources of interruption are eliminated. This is what is called a “reduction of the attack surface”.

**Prevention, detection and response.**

It’s best to assume that sooner or later, every company will be compromised by a cyberattack. At that moment, the time of detection and response to the incident is critical. A balance must be found between responding and recovering the service level for the business as soon as possible and analyzing the incident, the origin of the attack, and establishing measures to avoid it in the future.

As we said in the introduction, cyber-resilience refers to the ability of an organization to maintain its main goals and integrity against the threat of cybersecurity attacks. A cyber-resilient company is one that can prevent, detect, contain, and recover, minimizing the exposure time and the impact on business, of innumerable serious threats against data, applications, and IT infrastructure — and especially against the endpoint, where the organization’s most valuable assets reside, and against the integrity of user identity.

Although we are aware that total prevention is never guaranteed, companies should strive to minimize the cost of cyberattacks by strengthening prevention in pre-execution phases, preventing the attacker from executing malicious code on workstations and servers.

Equally important is complementing a cybersecurity strategy with quick detection and response in execution and post-execution phases to identify the damage, restore systems, and return operations to normal as soon as possible. Meanwhile, weaknesses and vulnerabilities can be newly detected in order to correct them and thus avoid the attack in the future.

**Implementing continuous processes to detect anomalies in user, endpoint, and application behavior.**

When it comes to minimizing the impact on business, the time that passes between a breach and its discovery, is the decisive factor in the overall cost of the incident.

Monitoring, visibility of the endpoint, and technologies that allow the automation of the detection and investigation can drastically reduce this amount of time. Detecting anomalous or malicious behavior in the profiles

of users, applications, and the devices, which are symptomatic of the presence of a hacker in the systems, is crucial.

**The management of cyber risk requires comprehensive and collaborative management.**

Many companies distinguish between physical security and IT security, between IT and Operations, between business continuity management and data protection, and between internal and external security. In the digital age, these divisions are obsolete. Scattered responsibility can put the entire organization at risk. Redundancies must be limited, and responses made quicker in order to increase resilience in general.

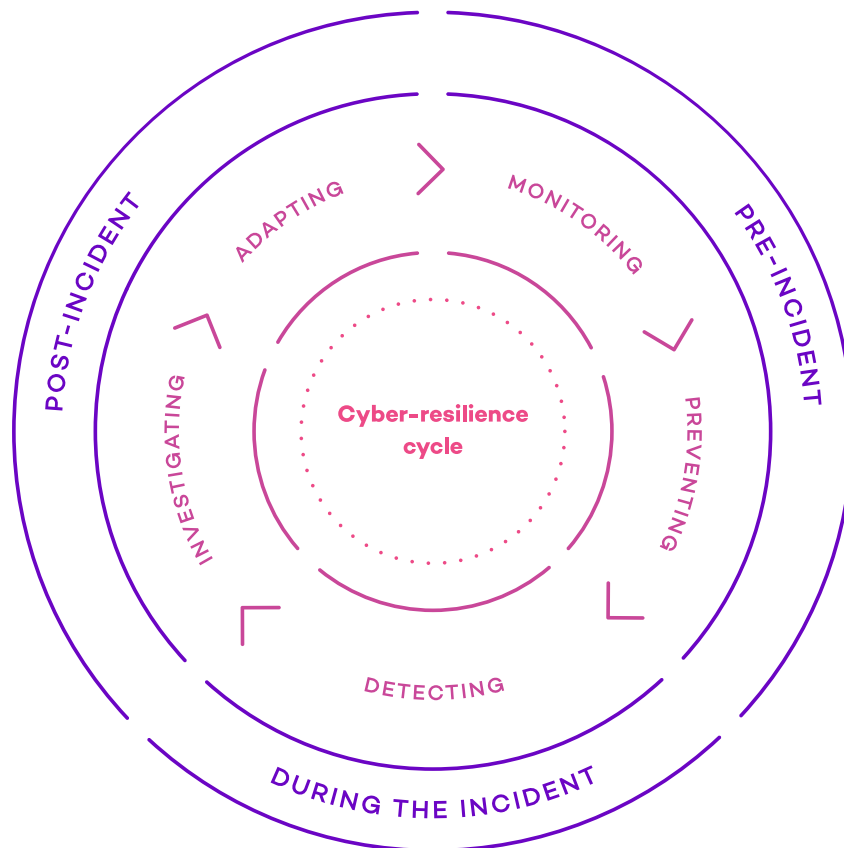


Figure 6. The cycle of continuous improvement of the cyber-resilience that every organization should develop and implement.

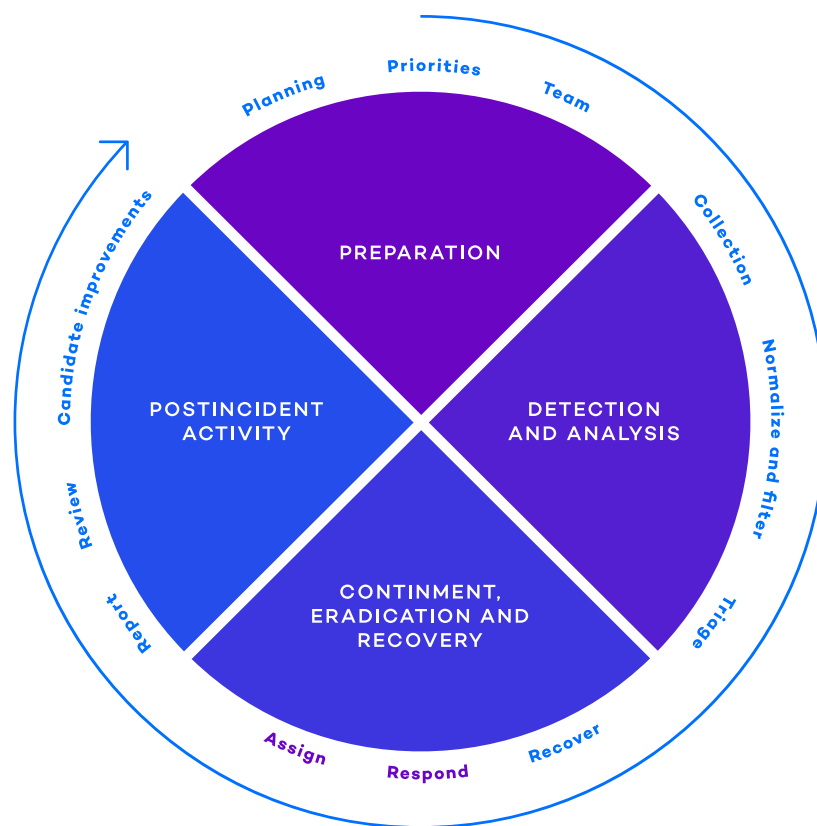


The following figure was taken from the Gartner report from January 28, 2018: “Improve Operational Resilience Through to More Collaborative Incident Response Process”. It illustrates the areas of the incident management and response cycle where collaboration and coordination is necessary — the boxes in blue — and the functions where the specific capabilities of each department, operations and security apply — the boxes in red

— with the aim of detecting and responding in the shortest time possible while identifying areas for improvement:

Companies that adhere to these principles tend to be much more resistant to attacks than ones that don't.

## Incident Handling



- Legend:
- Similar task and practices
  - Divergent task and practices

Figure 7. Coordination between Operations and Security teams when managing a security incident. Gartner: “Improve Operational Resilience Through to More Collaborative Incident Response Process”. January 25, 2018. Analysts: Matthew T. Stamper, Kenneth Gonzalez

## How does my company rate for cyber-resilience?

As part of the IBM and Ponemon Institute resilience study, “The Third Annual Study on the Cyber Resilient Organization”<sup>13</sup>, conducted this year, characteristics of organizations with a high degree of cyber-resilience were identified.

Companies are advised to evaluate their situation regarding these characteristics and take the appropriate measures to close the gap between where they are and where they should be. These measures are manifold, both in nature and in number. Adopting the appropriate technologies, solutions, and services offered by security vendors and service providers can get companies started right away and without requiring a large initial investment, and pays off in the short term by significantly reducing operating costs derived from incidents and data breaches.

Companies with a high level of cyber-resilience, are characterized by:

**Having a cybersecurity program with high levels of maturity**, totally or at least partially deployed throughout the organization and continuously improved.

According to the SANS Institute report “Behind the Curve? A maturity Model for Endpoint Security”<sup>14</sup>, where the maturity model is defined in terms of endpoint security, an organization in a state of high maturity is able to prevent cyberattacks before they can be executed. Or make changes in the systems that affect the endpoint, detect attacks that were able to bypass deployed security solutions, report on the status of the incident, and prevent the spread of new attacks in the company. In short, they have a security program deployed in the organization based on proactive defense, substantially improving the overall resilience of the organization.

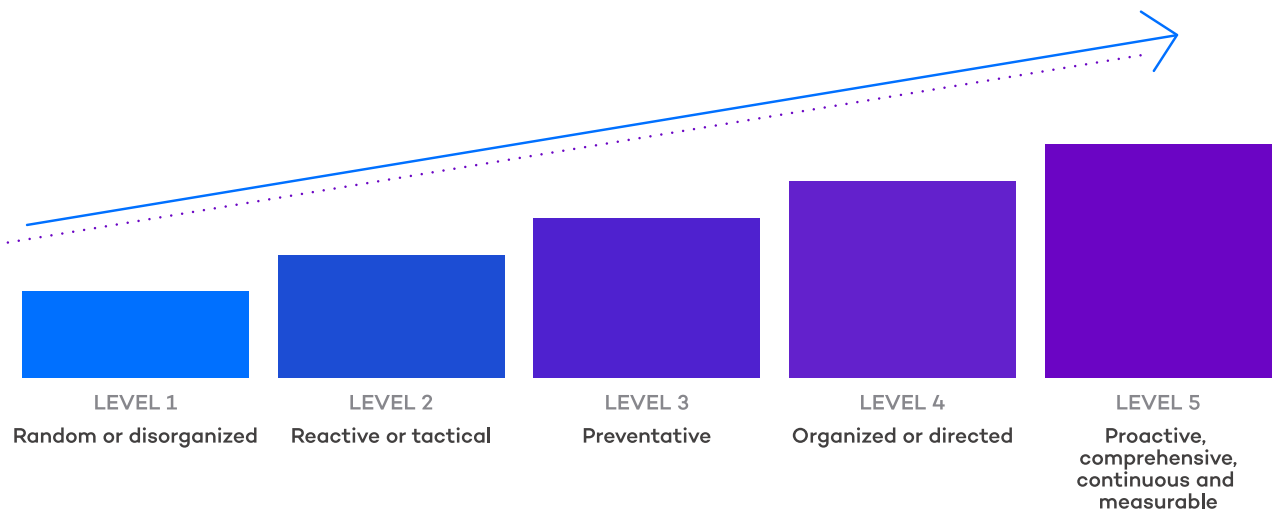


Figure 8. Maturity model of security on workstations and servers according to the SANS Institute, where the five levels of maturity are defined with respect to the security program developed and implemented.

<sup>13</sup> <http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study>

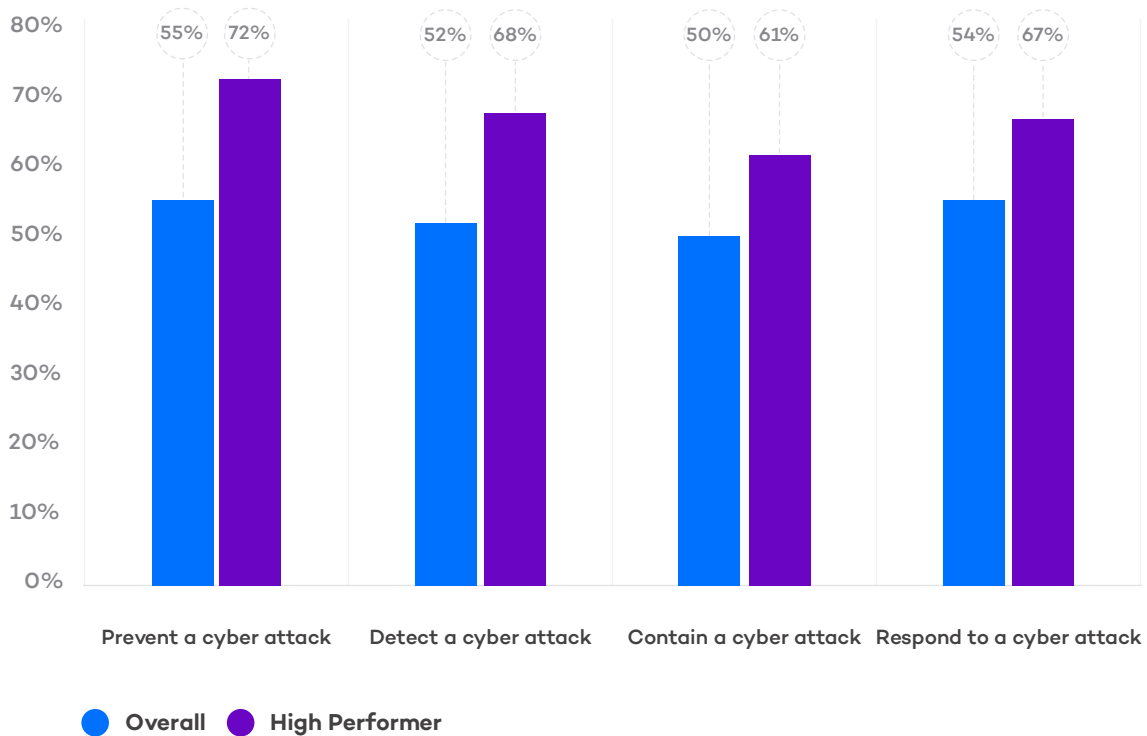
<sup>14</sup> <http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study>

**Highly cyber-resilient organizations have developed robust capabilities of prevention, detection, containment and recovery in a cyber-attack.**

As described by the Ponemon Institute study on resilience, the most resilient companies are those which have invested in the development of preventive, detection, and response capabilities.

**Figure 22. Organizations confident in preventing, detecting, containing and responding to a cyber attack**

1 = low ability to 10 = high ability, 7+ responses reported



**Figure 9. Ponemon Institute: relationship between cyber-resilience and capacity for prevention, detection, containment and response.**

**Highly cyber-resilient companies have developed a Cybersecurity Incidents Response Plan (CSIRP)**  
 This plan is based on continuous monitoring and event correlation using data collected by sensors on network devices and/or endpoints, as well

as mechanisms for detection, investigation and automated response and/or managed by security experts, or threat hunters.

**What best describes your organization's cybersecurity incident response plan (CSIRP)**

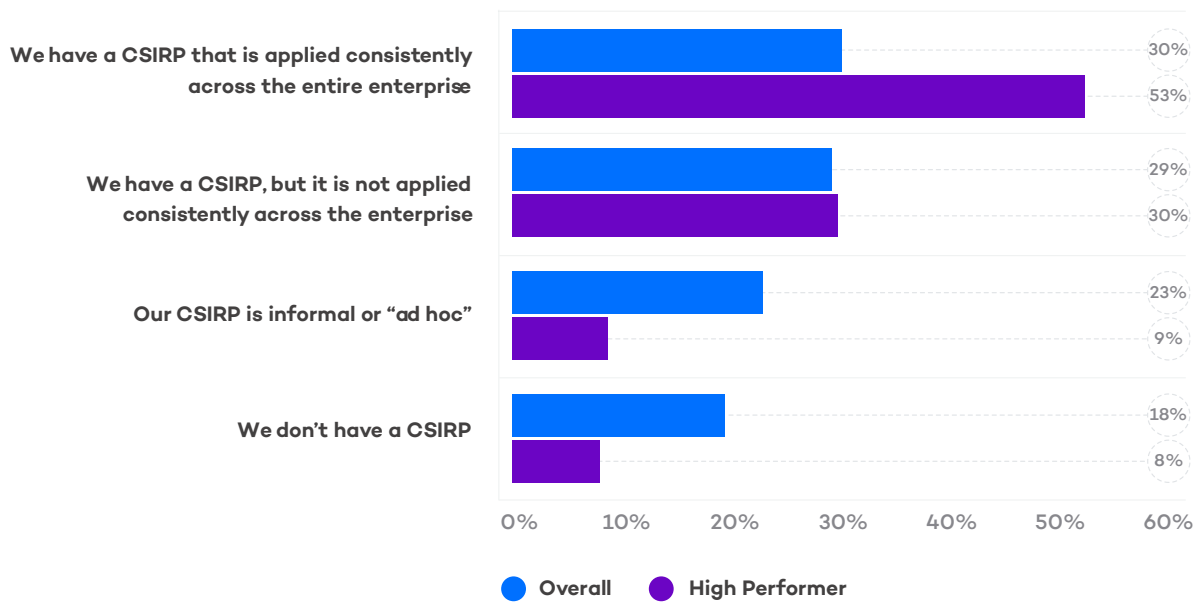


Figure 10. Ponemon Institute: relationship between cyber-resilience and the implementation of a response plan for cybersecurity incidents.

Moreover, almost all companies with a high level of cyber-resilience consider it essential to have, within the internal security team or through

an external SoC, highly qualified personnel in cybersecurity as part of the incident response plan.

**It is very important to have skilled cybersecurity professionals in their CSIRP**

1 = low ability to 10 = high ability, 7+ responses reported

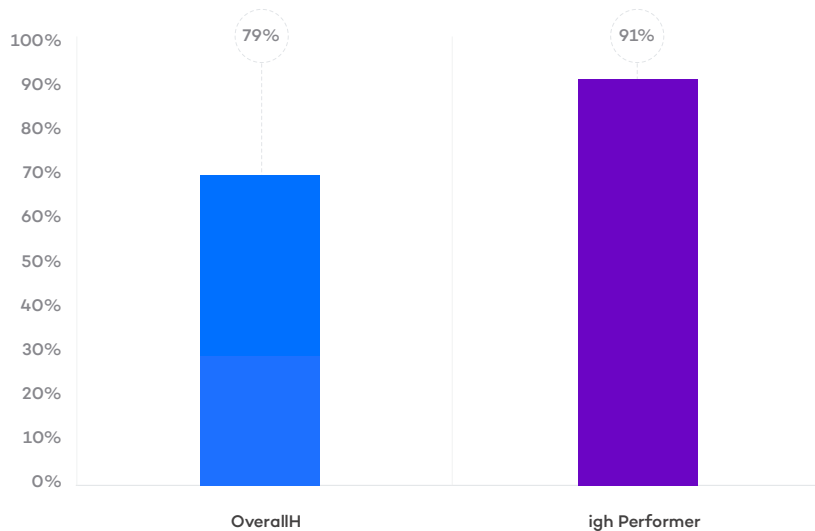


Figure 11. Ponemon Institute: relationship between cyber-resilience and the need to have highly qualified and specialized resources dedicated to cybersecurity

**Cyber-resilient corporate governance:** Managers at companies with high cyber-resilience are sensitive to the positive relationship that exists

between this factor and economic growth, as well as the strengthening of their company’s brand and reputation.

**Senior management’s awareness about the positive impact of cyber resilience on the enterprise**

Strongly agree and Agree responses combined

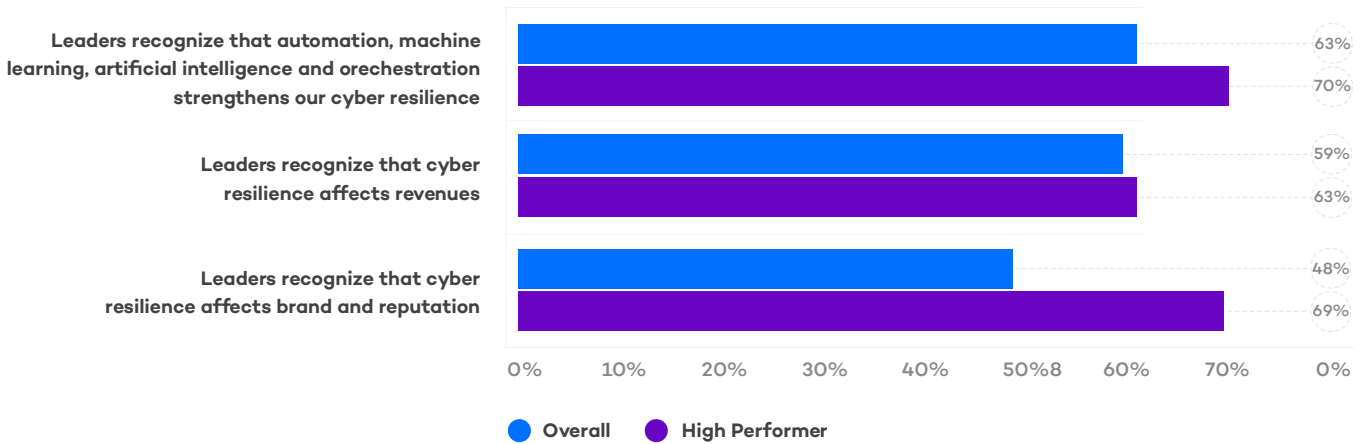


Figure 12. Ponemon Institute: The importance of senior management involvement in building a high level of cyber-resilience in companies.

## Conclusions

The digital transformation that is taking place in almost all aspects of our lives has a special importance when looking at the evolution of companies, organizations and public entities, interconnected devices, applications, tools, and productive processes.

From a competitive point of view, the search for optimization using new and improved instruments, means, capacities, and processes, is the origin of almost all initiatives in both the private and public sectors.

However, there is another aspect that we cannot ignore on the road to digital transformation: the transformation must also be deeply invested in security and business risk management.

Even more so, given the evolution in number and sophistication of threats. Cybercrime is an attractive and very lucrative business. Attackers have increasingly more and better resources — both technical and economic — which allows them to develop increasingly sophisticated attacks. All this results in more complex and dynamic threats, in addition to a greater number of attacks.

**Equifax**, CCleaner, WPA2, Vault7, CIA, KRACK, NSA, **WannaCry**, **Goldeneye/NotPetya**, Meltdown/Specter, **the election hacks...** These are some of the very recent protagonists of massive infections, theft, personal data leaks, ransomware attacks, hacked applications to launch attacks against an entire country or carry out attacks directed against large specific companies, and vulnerabilities that affect billions of devices.

With real cases like these, it is not surprising that 75% of companies (according to a recent survey by McKinsey<sup>15</sup>) consider that cybersecurity is a priority for the proper development of their activity. The “stress situation” described above

requires a reaction that involves a company-wide focus on the security program, which develops and strengthens a business attitude of cyber-resilience.

**Cyber-resilience** is the ability of an organization to maintain its primary goals and integrity in the face of the latent threat of cybersecurity attacks.

A cyber-resilient company is one that can prevent, detect, contain and recover, minimizing the exposure time and the impact on the business of countless serious threats against data, information and applications and IT infrastructure. Especially against devices, where the company’s most valuable assets reside. Reaching devices also means attacking the integrity of identities and users.

In order to become cyber-resilient, the new approach to security must cover at least the following points:

**1. Manage cybersecurity as a problem of corporate risk management**, not as an IT problem, **and adopt the stance of a “resilience cycle”**. The key elements of the cyber-resilience cycle include:

1. Prioritizing the most valuable assets of the organization.
2. Prioritizing, knowing and understanding the most relevant adversaries and threats for each organization.
3. Knowing and implementing the best defenses against current and potential threats.
4. Being prepared for a moment when adversaries can bypass all security technologies and detecting them, containing them and remedying their actions as soon as possible to minimize corporate damage.

<sup>15</sup> <https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world>

5. Adopting a crisis position which continuously and actively seeks threats, and detecting vulnerable points that can later be used by threat actors to reduce the attack surface.
  6. Managing at the corporate level any communication of a breach.
  7. Defining and constantly executing initiatives to minimize risk and reinitiate the cycle of continuous improvement in the management of corporate security.
2. **Strengthen the four key pillars: prevention, detection, Threat Hunting, and containment and response and reduction of the attack surface.**
  3. **Adapt continuously to the new techniques and tactics of hackers and other attackers.** Being resilient implies that this adaptation has to be carried out in the minimum time interval, at the maximum speed, even in real time.
  4. **Prioritize and mitigate risks at all levels of the organization.** Companies must take advantage of managed tools, products, and services that automate these functions to profile, catalog, monitor activity (human, data, and infrastructure), and learn from them so that security systems are predictive and accelerate the prevention and/or early detection of adversaries by reducing the level of organizational risk without incurring disproportionate costs, especially operational ones.
  5. **Manage cyber risk through comprehensive and collaborative management.**

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Panda Security.

© Panda Security 2017. All Rights Reserved.

#PASS2018