# DATA PRIVACY AND SECURITY TRENDS FOR 2018

An Industry Report from the

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org


With companies, governments and citizens facing a growing risk of being hacked, data security demands both defensive and offensive strategic solutions.

## DATA PRIVACY AND SECURITY TRENDS FOR 2018

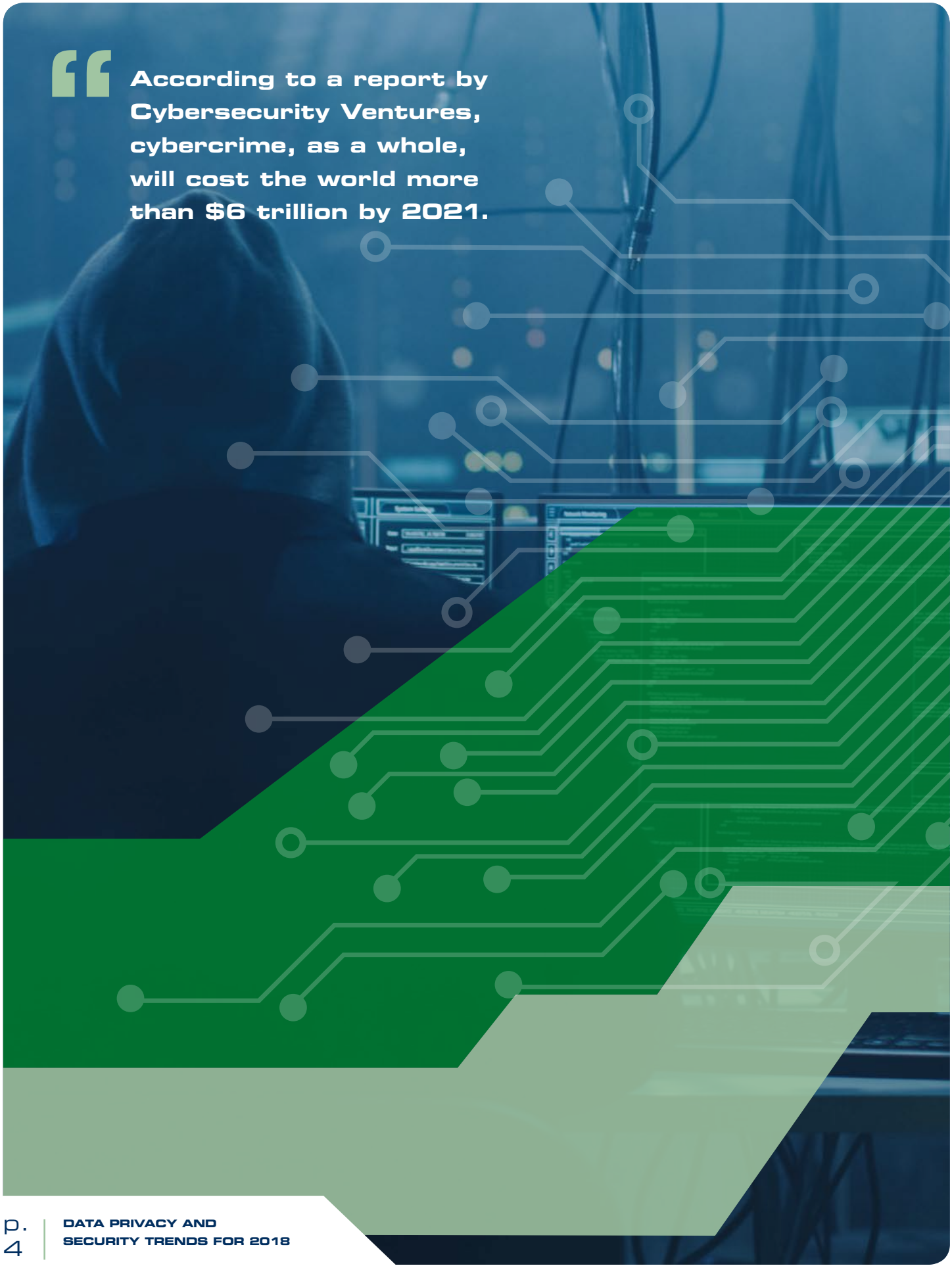
Data breaches are at an all-time high, with new and evolving technologies being used to instigate as well as prevent cyber attacks. With companies, governments and citizens facing a growing risk of being hacked, data security demands both defensive and offensive strategic solutions.

This paper explores some of the major data privacy and security trends for 2018 for professionals seeking an introduction to this critical issue.




**SIA Data Privacy Advisory Board**

This document was produced by the SIA Data Privacy Advisory Board. For more information about the board, visit our website at securityindustry.org or contact Ron Hawkins, SIA's director of industry relations, at (301) 804-4713 or rhawkins@securityindustry.org.



> According to a report by Cybersecurity Ventures, cybercrime, as a whole, will cost the world more than $6 trillion by 2021.

# Cybercrime Has Gone Mainstream

The year 2017 marked a time of great change in the technology sector, with frontier technologies such as artificial intelligence and blockchains creating their own micro-bubbles. With regard to data privacy and security, 2017 was the year that cybercrime went mainstream. For businesses, dealing with IP theft, malware and viruses is now the norm.

During the first six months of 2017, there were 918 reported breaches that compromised 1.9 billion data records, according to Gemalto, an increase of 164 percent compared to the previous year. From May through July 2017, a data breach at Equifax, one of the United States' three largest credit reporting agencies, exposed the personal information of 143 million Americans. Hackers gained access to credit card numbers, Social Security numbers, birthdates and other personally identifiable information.

Ransomware attacks are also soaring, rising from 3.2 million in 2014 to 3.8 million in 2015 to 638 million in 2016, according to SonicWall. In May 2017, a single piece of ransomware software called WannaCry claimed 200,000 victims in 150 countries. The U.S. government concluded that North Korea was responsible for the attack, illustrating that companies and institutions now face threats not only from criminals, but also from nation-states.

By the end of 2017, the global cost of ransomware was projected to exceed $5 billion. And, according to a report from Cybersecurity Ventures, cybercrime, as a whole, will cost the world more than $6 trillion by 2021.

Gartner predicts that part of this results from growing demands for application security testing, as part of the shift to DevOps, an engineering process that unifies software operation and development.

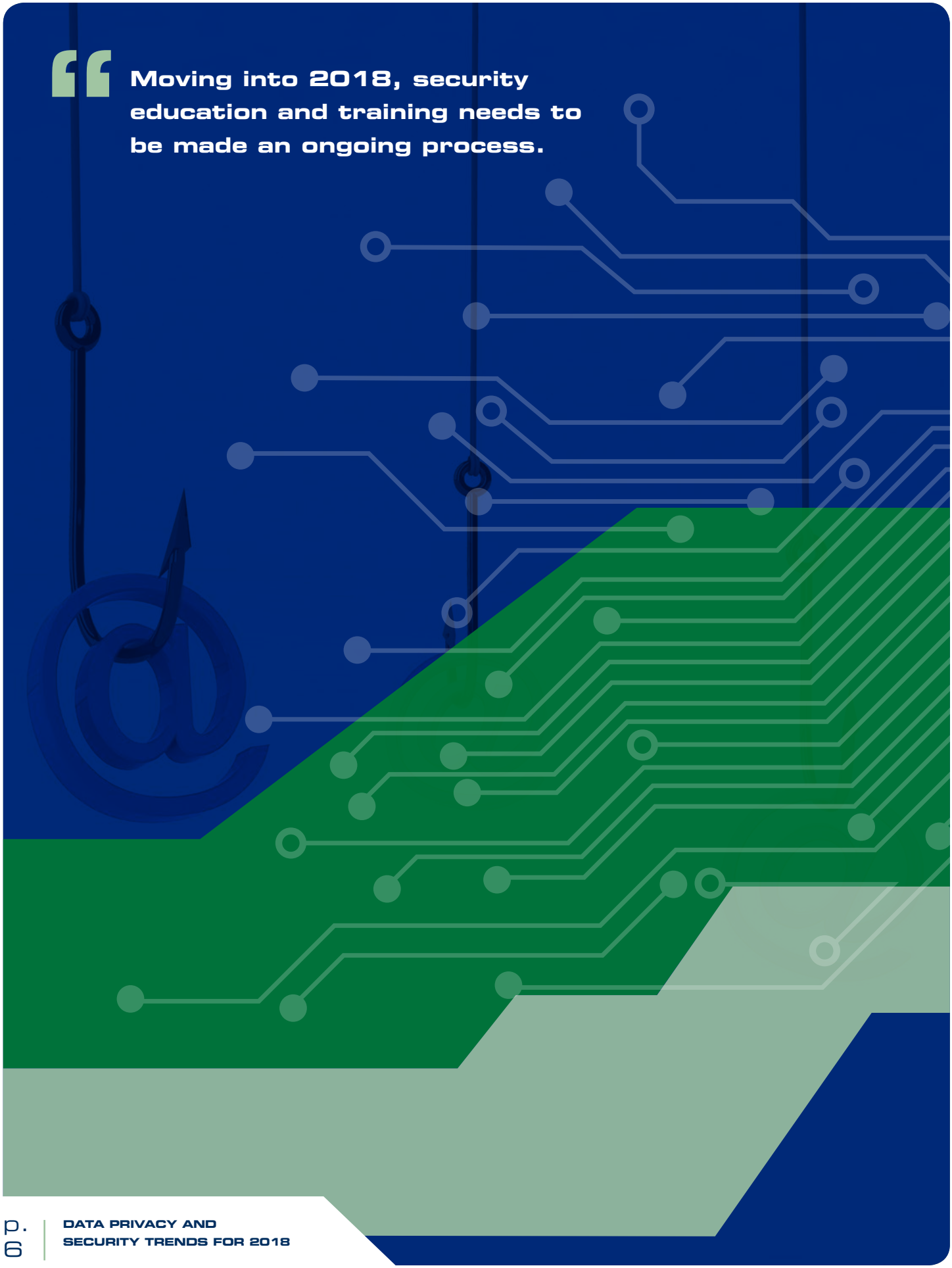
The increasing number of hacks and breaches has led to governments implementing new rules, such as the European Union's General Data Protection Regulation and Canada's Breach of Security Safeguards Regulations.

As cybercrimes continue to proliferate and laws meant to prevent these incidents take effect, new data security trends are emerging. To identify and explore these trends, we must first look at how different technologies and gaps in security precautions have gotten us here.

Ransomware attacks are soaring, rising from 3.2 million in 2014 to 3.8 million in 2015 to

**638**

**million in 2016**


Moving into 2018, security education and training needs to be made an ongoing process.

## Social Engineering and AI: The Evolution of Attacks

Many companies have put zero training into preventing or countering social engineering attacks, which account for 50 percent or more of all cybersecurity intrusions, according to Alan Silberberg, CEO of the digital and cyber advisor Digijaks. These attacks involve using phishing emails, phone calls and text messages, honey pot websites, fake social media accounts, and fake URLs to convince unsuspecting employees to provide information or access that is then exploited.

Moving into 2018, security education and training needs to be made an ongoing process. According to a report from the Business Continuity Institute, which surveyed 734 individuals in 69 countries, only 52 percent of companies conduct cybersecurity awareness-raising seminars and just 55 percent conduct regular exercises related to potential threats.

Making things even more difficult for companies, the use of artificial intelligence-based malware and AI-based responses is growing. Silberberg says that one of the biggest trends he expects to see in 2018 is the deployment of polymorphic malware, which uses AI to morph itself so it cannot be found. As soon as this malware is detected, it changes form and disappears.

"In the very near future, AI-driven malware is going to be a much larger driver of cybersecurity because it's a driver of tools that criminals use," Silberberg said.

According to a survey covering 69 countries, only

**52%**

of companies conduct cybersecurity awareness-raising seminars


Companies need to be investing in 24/7 AI-driven defenses, but they have to be combined with humans.
– Alan Silberberg, Digijaks CEO

# The Rise of the Machines

In 2018, more security vendors will likely integrate artificial intelligence into their products to improve their ability to detect cyberthreats. Just as some phishing scams already use AI to generate social engineering campaigns, security products are integrating AI to enable more efficient threat detection. ABI Research forecasts that machine learning in cybersecurity will boost big data, intelligence, and analytics spending to $96 billion by 2021.

But threat detection will only go so far, as it is a reactive measure. If 2017 has shown enterprises anything, it is that organizations must be proactive in identifying and thwarting potential attackers before they strike.

Automated threat-seekers—dubbed robo-hunters by Dimension Data Group—are AI-based programs that survey an organization's environment and devices for potential threats.

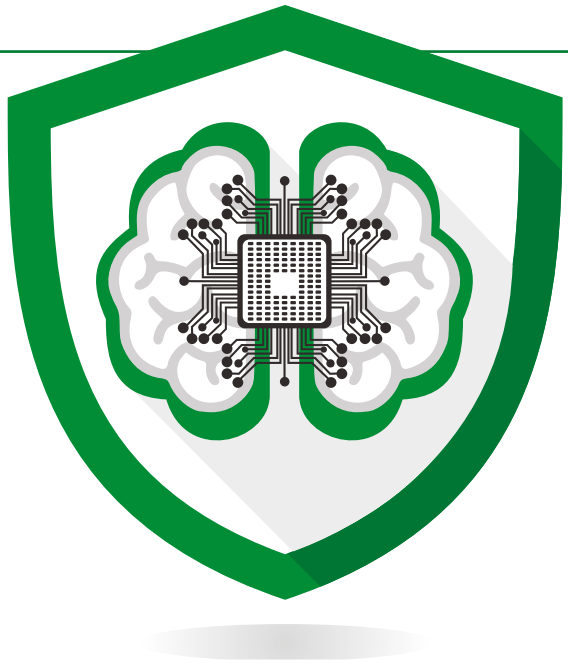
Steve Grobman, CTO at McAfee, says that AI will not make human cybersecurity experts obsolete, but the technology will reduce the number of personnel needed and will allow them more time and space to improve their efficiency and effectiveness. The tirelessness of machines, meanwhile, means that protective measures—like the threats they guard against—are always on.

"Companies need to be investing in 24/7 AI-driven defenses, but they have to be combined with humans," Silberberg said. "There has to be some level of analysis, as well. This is not a 9-to-5 attack mode thing anymore. This is 24/7."

ABI Research forecasts that machine learning in cybersecurity will boost big data, intelligence, and analytics spending to

**$96**

billion by 2021



> **[The Equifax breach is] a perfect example of what can happen when an organization doesn't have up-to-date software.**
>
> — Arlo Gilbert, Meta Saas CEO

One area, in particular, where security demands a combined effort from humans and AI is the cloud. The size of the cloud-based security services market is expected to nearly double from $4.84 billion in 2016 to $8.92 billion in 2020, according to Gartner, and many IT security experts say that artificial intelligence and automation are the best ways to monitor activity over different channels.

While machines can manage platforms well, people need to do their part, and better cloud security practices typically come down to company culture and common sense.

One approach for cloud industry services that could be beneficial is to create and follow an industry standard. Many high-profile breaches resulted not so much from hacks as from someone leaving information exposed on a server. For this reason, Silberberg suggests that major cloud players create a standard and enforce security education and training.

"Amazon could institute a cybersecurity protocol that every company has to adhere to before being allowed to have a server," he said. "That includes a certain base level of training or cybersecurity support built in, so that the configurations that are leaving a lot of these companies vulnerable with information being left out in the blue can be safer."

Arlo Gilbert, cofounder and CEO of Meta SaaS, a cloud application management platform, agrees, adding that managing and updating tools is crucial for cloud security.

"Just take the Equifax breach," Gilbert said. "It's a perfect example of what can happen when an organization doesn't have up-to-date software."

With the proliferation of new devices and applications, management of these tools and the way they plug into a company's network is key for optimum security.

The size of the cloud-based security services market is expected to nearly double from **$4.84 billion in 2016 to $8.92 billion in 2020,** according to Gartner.

**Security best practices now need to address the fact that organizations have tools being used internally that may not have been vetted by the company.**

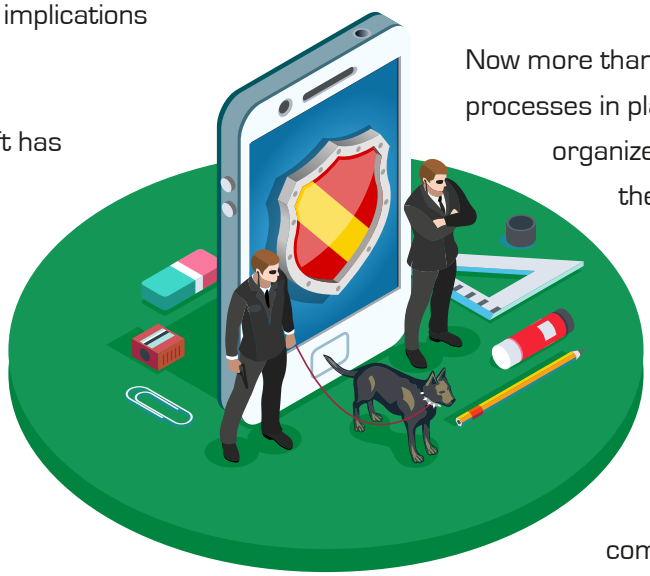
## Managing External Tools and Creating a Culture of Security

An additional trend in cloud security that creates challenges for companies is the move away from a "top-down" methodology.

"Once upon a time, there would be one entry point into an organization, like a LAN, and then people would go through a firewall," Gilbert said. "The CIO would control the computers people used and the applications people used."

The mobile revolution, though, brought with it the "bring your own device" (BYOD) movement, and many companies are still grappling with how to manage the security implications of this.

In the last five years, the shift has been into software as a service (SaaS) and cloud applications, which is similar to the move to mobile in that it has led to employees bringing their own software to work without first getting approval.



Security best practices, therefore, now need to address the fact that organizations have tools being used internally that may not have been vetted by the company. How do they do this? Gilbert says the answer is better governance.

"The biggest changes we've been seeing in cloud security is a move to improving governance and process," Gilbert said. "You don't need a massive alarm, as long as you don't leave your window open. You can affect your security positively by having some reasonably good processes around your people, software and hardware."

Creating a culture that embraces secure practices is critical, Gilbert adds. He advises that companies develop security guidelines for private and public cloud use, and utilize a cloud decision model to apply rigor to cloud risks.

Now more than ever, there is a need to have processes in place to identify, catalogue and organize who has access to data, where the data lives, and what software upgrades are needed.

And all of the processes and good governance must be executed from the first day of a person's employment to the last: A large number of leaks come from former employees who grab sensitive data on their way out.

"It's like not leaving your wallet on the seat somewhere," Gilbert said. "When employees leave an organization, the company needs to turn off their access to everything."

**More progressive organizations are marrying physical security and cybersecurity from a forensic security standpoint. How you respond to a physical breach and a data breach needs to be working hand in hand, as opposed to treating them as two separate incidents.**

—Zane McCarthy, Security Consultant

# The Intersection of Cybersecurity and Physical Security

Just as cloud security, specifically, and cybersecurity, generally, need better governance heading into 2018, physical security demands the same. Some argue, in fact, that with physical security equipment now commonly IP-enabled and connected to the Internet of Things, cybersecurity and physical security should be managed by the same entity within an enterprise.

Any device within a company that is connected to the Internet represents a possible vulnerability for that company. That is why connected devices, such as video surveillance cameras—some of which enabled the October 2016 DDoS attack that shut down large parts of the Internet—and HVAC equipment—which was the entry point for the attackers in the November 2013 Target hack—must be secured.

Physical security teams and cybersecurity professionals need to monitor all users of both the network and the physical space. Companies must track which computers and servers employees and consultants use and what information and controls they have clearance to access. Without a combined effort between physical security and cybersecurity operations, searches for attackers will likely be incomplete and ineffective.

Security consultant Zane McCarthy stresses that physical and cyber threats can no longer be viewed distinctly.

"More progressive organizations are marrying physical security and cybersecurity from a forensic security standpoint," McCarthy said. "How you respond to a physical breach and a data breach needs to be working hand in hand, as opposed to treating them as two separate incidents."

Shifts in company culture and governance are becoming even more crucial for companies handling large data sets as the enforcement date of the European Union's General Data Protection Regulation draws near. While it is an E.U. rule, this regulation will have an impact on organizations around the world.


> **Noncompliant organizations could face massive fines, whether they are in the E.U. or are based elsewhere but improperly process personal data within an E.U. country.**

# Understanding the General Data Protection Regulation

The General Data Protection Regulation (GDPR) was created in response to the rapidly-evolving challenges posed by the 21st century information economy to the preservation of individual privacy and autonomy. The regulation states that it "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" and "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."

Enforcement of the GDPR will begin on May 25, 2018. At that point, noncompliant organizations could face massive fines, whether they are in the E.U. or are based elsewhere but improperly process personal data within an E.U. country. The determining factor will be not where the organization is, or where the person connected to the information is, but whether the data is processed within E.U. borders.

The regulation establishes strict mandates for the handling of personal data, requiring, among other things, that:

- Information be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"
- Breaches be reported within 72 hours of detection
- Personal data be erased upon request ("the right to be forgotten"), though certain legal and public interest exceptions allow for the possibility of there being "overriding legitimate grounds" for the data to be processed
- Firms only process personal data under certain conditions (when a person gives consent, when it is necessary for the performance of a contract, when it is needed for compliance with a legal obligation, etc.)

In addition, if an organization acquires personal data based on an individual's consent, the opt-in declaration must be written "in an intelligible and easily accessible form, using clear and plain language."

The penalties for not adhering to the regulation are significant. For the most egregious violations, a company found to be in violation could be fined as much as 4 percent of its global gross revenues or $20 million, whichever is greater.

"Overall, GDPR is pushing everyone in the right direction," Silberberg said. "It just may cost a lot of money to get there."


From digital identities to genomic metadata and beyond, startups are storing the personal information of users on private blockchains and creating a new personal data economy.

## Decentralizing Data Storage with Blockchains

While the GDPR is enhancing the digital civil rights of consumers, it does not address the fact that traditional centralized models of data storage are being replaced by blockchains—immutable, decentralized ledgers on which transactions and contracts are public, distributed and verifiable.

Cryptocurrencies have increased awareness of blockchains, which were originally created to record Bitcoin transactions. Today, blockchains are being used in situations where multiple parties need to share and secure information with each other without a middleman. Blockchains are ideal for instilling trust, as one complete copy of the chain shows that every transaction is held by the entire network. If someone attempts to break the chain, they can be easily identified.

Because of the highly secure functionality of blockchains, many of their features are being used in solutions for security problems across a number of industries and segments, including but not limited to finance, health, corporate social responsibility, and government.

Because all blockchain transactions are accessible and transparent to all participants, it is possible for businesses to use blockchains in corporate security settings. One practical use in a corporate scenario is using blockchains to detect suspicious online activity and isolate the connection. Other cybersecurity uses for blockchains that are expected to emerge in 2018 involve cryptography used to secure emails, websites and messaging applications.

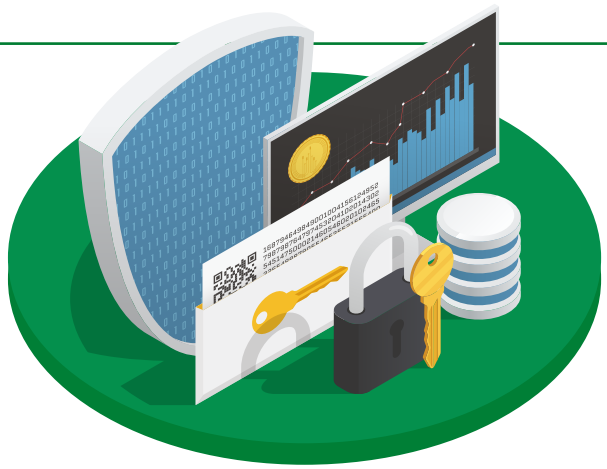
As for personal data, blockchains are being used to enable individuals to manage and control their identity. From digital identities to genomic metadata and beyond, startups are storing the personal information of users on private blockchains and creating a new personal data economy.

The Illinois state government has started testing a blockchain-based system for the digitization of birth certificates. In collaboration with blockchain identity startup Evernym, participants in the pilot program are testing tools that will allow parents and doctors to register the birth of babies on a permissioned blockchain.

One practical use in a corporate scenario is using

**BLOCKCHAINS TO DETECT SUSPICIOUS ONLINE ACTIVITY**

and isolate the connection.




**Differential privacy allows companies to collect user data in a format that lets it identify patterns of consumer behavior without violating anyone's privacy.**

## A New Technique: Differential Privacy

Just as governments are seeking to provide more data privacy to their citizens, companies are looking into new methods, as well.

The value to businesses of knowing as much about their customers as possible is not going to fade, but neither is the push for personal data security. Enter differential privacy, an approach that has become a standard for protecting individual information in large databases.

Apple and Uber, among other companies, have each announced that they are practicing differential privacy, which is essentially the statistical science of learning as much as possible about a group without knowing anything about specific individuals. Ideally, differential privacy allows companies to collect user data in a format that lets it identify patterns of consumer behavior without violating anyone's privacy.

According to Uber's security department, data analyses do not even reveal whether a given individual appears in the data. For this reason, differential privacy provides an extra layer of protection against re-identification attacks, as well as attacks using auxiliary data.

As data breaches continue and as more regulations like the GDPR are implemented, differential privacy may be used more widely throughout the tech industry, as well as in other sectors that make use of consumer data.

Differential privacy provides an extra layer of protection against **reidentification attacks,** as well as attacks using auxiliary data.

# Recommended First Steps

Given the rapidly evolving risks and the staggering costs—both financial and reputational—if such threats are not defeated, what can companies do to ensure the security and privacy of their data? Several leading organizations have published recommendations.

Cisco, for example, identifies six key components in its Data Protection Framework: policies and standards, identification and classification, oversight and enforcement, data risk and organizational maturity, incident response, and awareness and education.

The Ponemon Institute, meanwhile, calculated in its "**2017 Cost of Data Breach Study**," which was sponsored by IBM, how various factors affect the per capita cost of a breach. The five factors that reduce the cost the most are:

- Incident response team
- Extensive use of encryption
- Employee training
- Business continuity management involvement
- Participation in threat sharing

The factors that increase the cost the most are:

- Third-party involvement
- Extensive cloud migration
- Compliance failures
- Extensive use of mobile platforms
- Lost or stolen devices

Across the many sets of guidelines, some common themes emerge. The following recommendations provide a baseline for data privacy, with links provided to more extensive guidance.

## MAKE SECURITY A PART OF EVERY DECISION

The Federal Trade Commission, in a June 2015 list of **lessons learned** from more than 50 breach-related agency actions, stated, "Start with security. Factor it into the decision making in every department of your business—personnel, sales, accounting, information technology, etc. Collecting and maintaining information 'just because' is no longer a sound business strategy. Savvy companies think through the implication of their data decisions. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road."

## GUARD AGAINST INSIDER THREATS—BOTH INNOCENT AND NOT-SO-INNOCENT

The "**2017 Data Breach Investigations Report**" from Verizon found that, in 2016, 25 percent of breaches involved insiders. In addition to this direct threat from employees, though, 14 percent of breaches involved privilege misuse, 43 percent were social attacks, 51 percent involved malware—two-thirds of which were distributed through email attachments—and 81 percent leveraged stolen or weak passwords. Some first steps to address these issues include requiring the use strong passwords, using multi-factor authentication, and applying the "principle of least privilege" when provisioning access.

*Create a culture of risk awareness and mitigation that extends to employee-owned devices.*

The International Association of Privacy Professionals published an **article** in June 2016 that stated, "Establishing a strong company culture and improving training programs with the involvement and enforcement of executives will emphasize the importance of reducing the risk of a data breach or security incident, saving companies from their biggest security threat—their own employees. With time, employees can even become a security asset by detecting potential attacks and alerting the security teams so they can take action."

*Train employees to defeat social engineering attacks.*

The SANS Institute, which advises implementing a training program that accounts for individual employee personality traits, as identified through testing, noted in an April 2016 **whitepaper**, "Electronic-based social engineering is potentially easier to train for as it happens more regularly and users can be taught not to open emails from anyone they do not recognize. But human-based social engineering, for example a phone call from a seemingly trustworthy person or even letting a stranger tailgate into the office simply because they have on what appears to be an official uniform can be a much more serious threat. Yet the reality is most organizations do not properly train their employees to recognize these potential hazards."

*Log and track usage to identify bad actors within an organization.*

The CERT Insider Threat Center at Carnegie Mellon University in December 2016 published a 175-page "**Common Sense Guide to Mitigating Insider Threats**" that identifies 20 practices intended to prevent and detect this risk: "By building an effective insider threat program, an organization can significantly reduce its exposure to the problem and prevent the most damaging insider attacks. The program must implement a strategy with the right combination of policies, procedures, and technical controls. Management from all areas of the organization, especially at the executive level, must appreciate the scale of the problem and work together to modify the organization's business policies and processes, culture, and technical environment.

## IMPLEMENT EFFECTIVE CYBERSECURITY

Many resources are available that outline the basics of cybersecurity, including the "**Beginner's Guide to Product and System Hardening**" and "**Recommendations for Initiating an Enterprise Cybersecurity Strategy**," both from the Security Industry Association's Cybersecurity Advisory Board. In addition, physical security teams and cybersecurity teams should work together. In 2009, Scott Borg, director of the U.S. Cyber Consequences Unit, said, "As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one. The convergence of cyber and physical security has already occurred at the technical level. It is long overdue at the organizational level." Yet, nearly a decade later, the two fields often remain separate, increasing the vulnerability of both.

## MANAGE THE RISK RELATED TO THIRD-PARTY POLICIES, PRACTICES AND SYSTEMS

A September 2017 report on "**Data Risk in the Third-Party Ecosystem**," which was produced by the Ponemon Institute and sponsored by Opus, found that "the two most effective practices that when deployed reduce the likelihood of a breach are the evaluation of the security and privacy practices of third parties ... and an inventory of all third parties with whom the organization shares information."

## HAVE A PLAN IN PLACE TO RESPOND TO BREACHES

An incident response plan enables organizations to contain damage and costs by reacting to security incidents in as timely and effective a manner as possible. The National Institute of Standards and Technology, in its December 2016 "**Guide for Cybersecurity Event Recovery**," states, Planning ... enables the organization to explore 'what if' scenarios, which might be largely based on recent cyber events that have negatively impacted other organizations, in order to develop customized playbooks. Thinking about each scenario helps the organization to evaluate the potential impact, planned response activities, and resulting recovery processes long before an actual cyber event takes place. These exercises help identify gaps that can be addressed before a crisis situation, reducing their business impact."

## STAY CURRENT ON REGULATORY AND COMPLIANCE ISSUES

Several federal laws impose privacy requirements—such as the Health Insurance Portability and Accountability Act (HIPAA) in the health care sector and the Gramm-Leach-Bliley Act in the financial sector—and some states have their own mandates. (See the list of state **Security Breach Notification Laws** from the National Conference of State Legislatures and the November 2017 "**Data Breach Charts**" from BakerHostetler.) In addition, companies that do business overseas need to be aware of local laws. For example, if a company processes personal data in the European Union, it must ensure that the required structures, policies and procedures are in place before the General Data Protection Regulation goes into effect on May 25, 2018. The Information Commissioner's Office in the United Kingdom has published multiple **documents** on preparing for the GDPR and advises, "It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications."

## Conclusion

A surge in data breaches and impending threats are pushing enterprises to enter a brave new world of security measures. As emerging technologies like artificial intelligence are used in malware, the need for AI-driven security products is growing.

Despite these expanding threats, many companies are not sufficiently educating their employees about good cybersecurity and data privacy and protection practices. Implementing better governance and building a security-focused company culture is necessary for enterprises to protect their own data, as well as that of their customers. Security guidelines for private and public cloud use are paramount.

Moving forward, cybersecurity and physical security teams need to work together, since weaknesses in either area can be exploited to breach the other. This approach, along with other proposed process enhancements, is pushing companies toward a more proactive protective posture, especially as many firms prepare for the European Union's General Data Protection Regulation to take effect in May 2018.

In addition to AI and machine learning, blockchains may represent the next privacy frontier for industries and individuals. And all of these developments are leading commercial organizations to implement methods, such as differential privacy, that will allow them to leverage customer data for business purposes while ensuring that the data remain private and secure.

The threats to data privacy and security are significant, but so are the defensive measures that are available, with frontier technologies offering the potential of highly effective, proactive approaches. While 2017 was the year that cybercrime went mainstream, 2018 could be the year that cybersecurity culture becomes the default.

SIA
SECURITY INDUSTRY ASSOCIATION
securityindustry.org