Cyber Chief

Magazine

New Format

Ed.6

Data Security & Data Privacy: Finding the Right Path

Even more insights for cybersecurity professionals in each issue:

Cybersecurity by the numbers	Analysis of emerging trends	Advice from industry experts	Real-life stories

Ed. 6

Cyber Chief

Magazine

They say security is a journey, not a destination. But this journey is becoming increasingly complex. With entry barriers for cybercriminals lower than ever, cyberattacks so powerful that they can ruin a business, and security budgets that are always tight, how can we guarantee the security of our data and networks?

The answer is that we can't. Even if we had unlimited budget, perfectly trained IT specialists and security-savvy users, there are still risks that we can't foresee and therefore for which we have no adequate solution.

But it's not all doom and gloom. In this ever-changing landscape, the only approach that works is to be proactive. That means going beyond traditional vulnerability scans and basic compliance with regulations to treating security as a lifecycle that includes continual assessment, measurement, testing and improvement.

It all starts with understanding your data. This edition of Cyber Chief Magazine begins with the basics of data security and data privacy, and then covers the key strategies you need on the endless path towards securing your systems and your business. Plus, the magazine now covers broader changes to the cybersecurity industry, with new columns covering cybersecurity statistics, analysis of emerging trends, real-life cybersecurity stories and more. Join us in our quest for a deep dive into cybersecurity.

The Cyber Chief team
cyber.chief@netwrix.com

Contents

Cybersecurity: Facts and Figures

Focus

Analysis

Extra Security

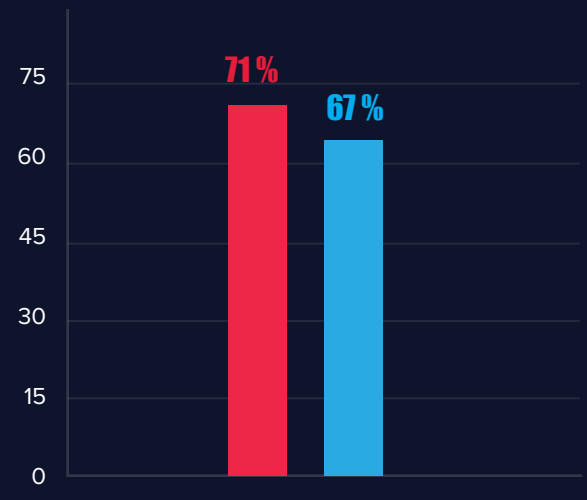
First-Hand Experience

Cybersecurity: Facts and Figures

Data Privacy and Data Protection

107 countries have enacted legislation to protect data and privacy

Source: United Nations Conference on Trade and Development



Americans occasionally or frequently worry about hacking of personal data

Americans occasionally or frequently worry about identity theft

Source: Gallup

ALL 50 U.S. states

have laws requiring organizations to notify individuals if their personal information is compromised

Source: National Conference of State Legislatures

31,456 records

The average size of a data breach in the U.S. in 2018

$ 7,91 million

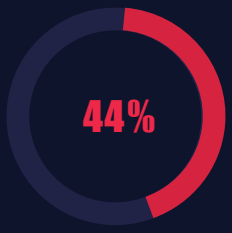
The average total cost of a data breach in the U.S. in 2018

Source: Ponemon Institute

8 in 10 U.S. adults

are concerned about the ability of businesses to safeguard their financial and personal information

Source:
American Institute of CPAs (AICPA)



of companies
don't know or are unsure
of what their employees are doing with sensitive data

Source: 2018 Netwrix IT Risks Report

TOP 3 issues

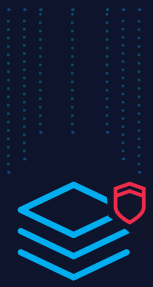
that led to data breaches:

Human error	29 %
Phishing attack	26 %
Password sharing	23 %

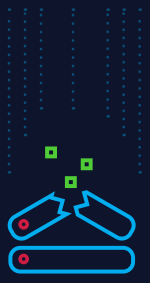
Source: 2018 Netwrix IT Risks Report

Risks

that organizations consider most critical:



41 %
Data breach



22 %
Data loss

Source: 2018 Netwrix IT Risks Report

SMBs

are not ready to address data security risks

Small businesses spend **< $ 500 per year** on cybersecurity

Source: Juniper Research

55 % of data breach victims in the previous year were SMBs (<500 employees)

Source: 2018 Netwrix IT Risks Report

Focus

Data Privacy vs. Data Security: What Is the Real Difference?

Earl Follis
Technology Evangelist and Consultant

The importance of cybersecurity has been growing exponentially over the last decade. Today, between persistent threats from cyberattacks such as malware and intrusions, accidental or intentional data loss, and data security regulations that impose stiff penalties on companies who ignore their data stewardship responsibilities, data security and privacy remain the hottest of hot topics for IT professionals worldwide.

However, even IT pros are not clear about the differences between data privacy and data security. This blog will explain what those terms have in common and what sets them apart from each other.

What Is Data Privacy?

Data privacy is ensuring that information is not accessed by unauthorized parties and that individuals retain control over their personally identifiable information (PII). Therefore, it is primarily concerned with the procedures and policies that govern the collection, storage and use of PII and proprietary corporate information, such as trade secrets, personnel and internal processes. PII stands out as highly sensitive information because of the civil and criminal liability companies and individuals face if they allow PII to be improperly exposed, whether due to overt actions or inadvertent data security lapses.

Ensuring data privacy requires more than a particular set of techniques or technologies. It also involves training every employee with access to sensitive data on the approved data protection processes. Just as an airplane pilot uses checklists to ensure that critical items are reviewed before flight and monitored during flight, IT pros must also be able and willing to use data privacy policies and other resources to ensure the privacy of PII and other sensitive data.

In particular, to ensure data privacy, IT pros should implement a set of guidelines, processes and procedures that spell out in detail how sensitive data is collected, stored and used by the company and its employees across all its systems. The purpose of this privacy policy is to ensure that all employees realize the importance of data privacy, understand how to help prevent improper exposure of data, and know how to deal with privacy issues and policy breaches.

Breaches of data privacy are no longer just embarrassing or inconvenient for organizations. Now, privacy laws like as HIPAA and the GDPR impose penalties for failure to safeguard the privacy of PII and other highly sensitive personal information. These compliance standards

can impose financial sanctions and even criminal charges for intentional and sometimes even unintentional exposure of PII. HIPAA is focused on the protection of healthcare-related personal data in the U.S., while the GDPR imposes a broader set of privacy standards and regulatory compliance requirements on any company that stores or processes the PII of EU residents.

What Is Data Security?

Whereas data privacy is implemented through a set of policies and procedures designed to safeguard the privacy of data, data security involves using physical and logical strategies to protect information from data breaches, cyberattacks, and accidental or intentional data loss. Specifically, data security is the technologies and techniques that companies use to prevent:

- Unauthorized access
- Intentional loss of sensitive data
- Accidental loss or corruption of sensitive data

Examples of measures for ensuring data security include resilient data storage technologies, encryption of data both at rest and in motion, physical and logical access controls that prevent unauthorized access, data masking, and secure elimination of sensitive data that is no longer needed. Specific techniques include multi-factor authentication, multiple layers of access control at the network and application layer, and the detection and isolation of unauthorized devices as soon as they attach to a network. Regular backups and tested disaster recovery plans are also a big part of data security.

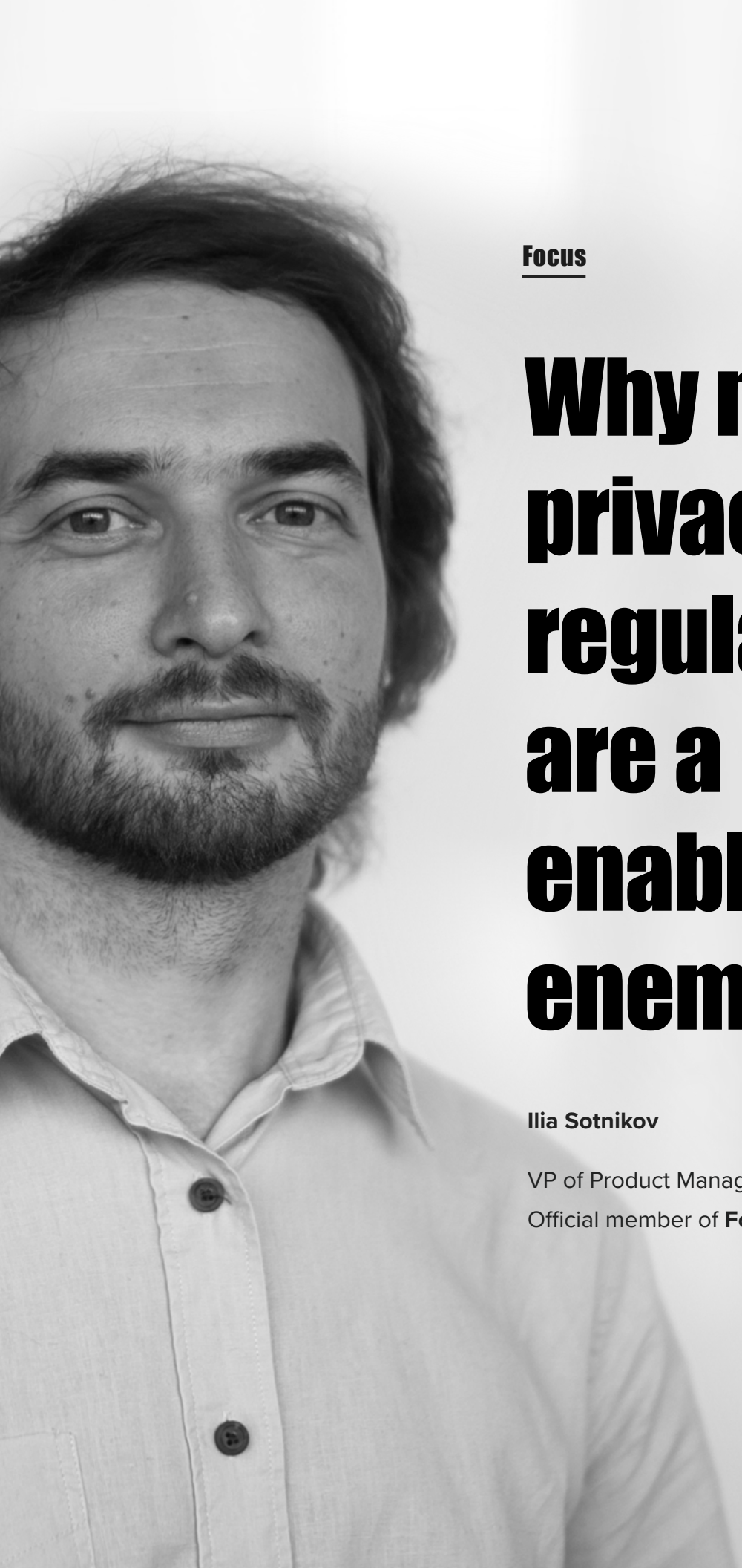
In short, data security is architected by a technologically sophisticated, holistic approach that secures every network, application, device and data repository in an enterprise IT infrastructure.

Data Privacy vs. Data Security

The best way to understand the difference between data security and data privacy is to consider the mechanisms used in data security versus the data privacy policy that governs how data is gathered, handled, and stored. Enterprise security of data could be effective and robust, yet the methods by which that data was gathered, stored or disseminated might violate the privacy policy. For example, a company might ensure that sensitive data is encrypted,

masked and properly limited to authorized access only. But if it collects that data improperly, for example, by failing to get informed consent from the owner prior to data collection, data privacy requirements has been violated even though data security remains unbreached.

Considering what's at stake for companies who are entrusted with the PII of customers and employees, implementing a privacy policy system is no longer just an admirable goal; it's a mission-critical aspect of every company's information security framework and operations. Before privacy compliance regulations were enacted, security practices were implemented on a best-effort basis. Now, the security systems that protect data have a direct impact on the risk management strategy of most companies. The protection of security data must now be a priority for every employee, not just IT pros.



Focus

Why new privacy regulations are a business enabler, not an enemy

Ilia Sotnikov

VP of Product Management at Netwrix,
Official member of **Forbes Technology Council**

Personal information (PI) is the future of business because it helps provide customers with a customized experience that leads them to buy more. However, companies can no longer collect personal data without restraint, given the growing wave of consumer rights advocacy and privacy regulations such as the CCPA, the GDPR and proposed U.S. federal laws.

Privacy legislation, with its strict requirements and enormous penalties, is often seen as a big stumbling block for business, but I perceive it as a huge enabler. Here are five ways that privacy regulations can help boost your business.

Benefit 1

Optimize business processes

Privacy regulations require greater transparency around data collection. For example, the CCPA requires businesses to disclose to individuals the "categories and specific pieces of personal information the business has collected" about them. To comply with these requirements, companies need to thoroughly audit all data they have, so they can understand what kind of information they store and why.

This is a brilliant opportunity to ask yourself questions like, "Why do we collect this data?", "Do we use it efficiently?" and "How else can we use it?" Getting a deeper understanding of data flows will provide more visibility into your business processes and help you optimize them or find new ways of leveraging the data you have gathered (for example, by providing more personalized experiences).

Benefit 2

Improve data management and achieve cost efficiencies

Another question to ask yourself after auditing your data is, "Do we really need all this data?" Most likely, you don't need it all. Thus, regular audits for the sake of compliance will actually enable your company to prune out unnecessary data, such as redundant, obsolete and trivial (ROT) files, that have no value to your business. By cleaning up repositories, you can slash costs on data management and storage, get more predictable bills if you store data in the cloud, and allocate your budget more wisely.

Benefit 3

Create a global knowledge base for employees

Privacy laws, especially the CCPA and the GDPR, grant consumers certain types of control over the data that businesses hold on them, such as the right to view the data and the right to be forgotten. To handle these requests efficiently, you need to be able to quickly find the relevant data, which requires ensuring your repositories are well organized and making the data globally indexed and searchable. And achieving that usually requires investing in technologies such as data classification and enterprise search software.

However, it wouldn't be cost efficient to spend time and money licensing and deploying this technology just to satisfy data subject requests once in a while. That would be buying a Porsche just to drive your children to school down the block. Instead, you can use the tools to reorganize and index not just consumers' PI, but all the data you have, or at least all the data that business employees might need. This way, your company will improve its corporate memory. Moreover, employees will be able to more efficiently find the data they need, so they won't miss business opportunities and will keep contributing to the company's long-term growth.

Benefit 4

Earn loyalty and trust

Another way to benefit from privacy legislation is to step up and voluntarily extend privacy requirements to all of your clients, not just those who are protected by the CCPA (California consumers), the GDPR (EU residents) or other standards. By meeting customer demands for data privacy globally, your business will create a stronger bond between your brand and clients that will give you a competitive advantage and help stand from the competition.

For example, you can eliminate annoying formal statements and cookie notifications that clients must assent to. Instead, show that you are eager to provide them with a clear privacy policy statement that explains how they can benefit from entrusting their PI to you and the measures you take to secure it. After all, when people are becoming increasingly suspicious about their privacy, the best response is to be honest and straightforward.

Benefit 5

Revamp your security strategy

The cost of data breaches and business downtime due to theft or loss of critical data continues to grow. Another benefit of privacy legislation is that it drives companies to overhaul their security policies. Indeed, it is almost impossible to protect regulated data only and leave the rest of IT infrastructure out of scope. Therefore, your company will have no chance but establish stricter control over activity across the entire IT environment, initiate solid data protection workflows and better understand IT risks. In the long run, that will help you reduce the risk of security incidents and business disruptions.

There's no doubt that achieving compliance with data privacy laws is stressful and resource-intensive, but don't be shortsighted. Adhering to data privacy standards is more than marking a checkbox — it is a way to greatly boost your business, stay ahead of the competition, and be a leader in meeting the global demand for corporate respect for human privacy.

Analysis

One year into GDPR

Ryan Brooks
Cybersecurity Expert, Netwrix Product Evangelist

Which patterns are the most frequent?

It has been a year since the General Data Protection Regulation (GDPR) came into effect, following years of discussion about data security fit for the digital age. One of the most stringent regulations to date, the GDPR applies to every business or public body that collects, processes or stores the personal data of EU residents. This includes not just every employer in the EU but every organization anywhere in the world that offers products and services to EU residents, as well as companies that process their personal data on behalf of other organizations. Because of its global reach, the GDPR has led to massive change in personal data protection, both within the EU and beyond.

The European Data Protection Board (EDPB) reports that during the first year since the GDRP went into effect, over 89.000 data breaches were logged and 446 cross-border cases were investigated by data protection authorities. In addition, the European Commission notes that the number of queries and complaints from individuals about the security of their data is rising, which suggests an increasing public awareness about the data protection rights afforded by the GDPR.

Another significant impact of the GDPR is that it helping to reveal how data is processed by internet giants, social media platforms and companies in other industries — a topic people everywhere have a lot of concerns about. For example, in its Annual 2018 report, the Irish Data Protection Commission (DPC) stated that it has opened inquiries into the data-processing activities of a number of multinational internet and technology companies based in Ireland, including Facebook, Apple, Twitter, LinkedIn, WhatsApp and Instagram.

GDPR non-compliance cases: What we've learned

An EDBP report covering the first nine months after the GDPR took effect reveals that regulators in 11 European countries imposed more than €56 million in fines. Most of this amount comes from a single sanction — the massive €50 million fine imposed on Google by the French data protection authority.

That is the biggest GDPR fine so far, but it's difficult to say how long Google will retain that dubious distinction. There are ongoing investigations into several serious data privacy violations, with the fines yet to be announced. One of them is a data breach at British Airways, investigated by the UK's information commissioner's office (ICO). Under the

GDPR, the company could be fined up to 4% of its global annual turnover, which would be a fine of €560 million — an order of magnitude larger than Google's penalty.

There also have been numerous enforcements involving smaller organizations with much lower fines. That suggests that authorities largely regarded the first year as a transition period for alerting companies and supporting them on their way to GDPR compliance, rather than chasing down every infringement and imposing maximum penalties.

Nevertheless, a number of organizations have already been slapped with significant GDPR fines. Here are some of their stories:

Failure to inform individuals that their data would be processed

Who: Unnamed data controller in Poland
When: March 2019
How much: €200.000

Violation: Under the GDPR, individuals have a right to be informed about the collection and use of their personal data. The organization in this case did properly inform the 90,000 people in their customer base whose email addresses they had — but it did not directly contact the other 6 million people for whom they didn't have email addresses, citing high operational costs. Instead, the organization chose to present the information about data collection and use on its website.

Key takeaways: Regulators found this approach insufficient, noting that the company had other contact details, such as phone numbers and physical addresses that it could have used to directly contact customers. The regulators also deemed the infringement intentional because the company was aware of the obligation to directly inform individuals and there was no attempt or even a declared intention to end the infringement.

The GDPR's influence on regulatory systems outside the EU

Since the GDPR came into effect, we have seen similar laws enacted around the world. According to the United Nations Conference on Trade and Development (UNCTAD), over 100 countries now have data protection laws in place. Brazil's new regulation even has a similar name: General Data Protection Law (GDPL). Over the next few years, we expect to see more enforcement regarding international data exchanges.

The EU is working to introduce the ePrivacy Regulation, which will replace ePrivacy Directive 2002/58/EC and complement the GDPR by regulating privacy with respect to electronic communication services, including the use of metadata and cookies.

Data privacy is also being addressed in the U.S. For instance, the California Consumer Privacy Act (CCPA), which has a lot in common with the GDPR, comes into effect on January 1, 2020. Massachusetts is upgrading its data breach law to include new requirements for businesses that collect the personal data of state residents, and Oregon is working on amendments to strengthen cybersecurity laws for organizations that suffer a data breach.

What experts say about the impact of the GDPR

We asked several experts how the GDPR has impacted businesses, and here is what they said:

Douglas Crawford, digital privacy expert, ProPrivacy.com

Arguably the biggest win is that GDPR has forced companies to think carefully about user consent and users' right to privacy. In reality, it will take some years for the full benefit to consumers to become apparent, but the final result should benefit ordinary internet users everywhere. Because taking a two (or more) tiered approach to user privacy is wildly impractical, companies have been forced to extend the privacy benefits of GDPR to all their customers, regardless of whether or not they live in the EU.

Although the first year has been dubbed a "transition year," GDPR has so far achieved notable success when it comes to data breach reporting. Within the EU, such reports almost doubled in the first eight months since GDPR was introduced. This is likely to put pressure on the U.S. government to institute similar laws on a federal level, rather than relying on an inefficient morass of state-level legislation that results in low levels of self-reported data breaches.

European regulators are likely to take a more muscular approach to enforcement of GDPR in the coming years. It makes sense to start with cleaning up their own backyard, but once this is done, it is almost certain the regulators will turn their attention more fully onto international firms who do business in Europe.

Monica Eaton-Cardone, co-founder and COO, Chargebacks911

As a global entrepreneur, I've noticed that many

companies have hired lawyers to assist with their data. When GDPR came into effect, people became more aware of the importance of protecting their data.

Although GDPR helped some businesses grow, there were thousands of complaints with regards to the lack of proper transparency, which wasn't a surprise. After all, at the time GDPR went live, few merchants had the infrastructure in place to parse data with as much detail as GDPR demands, and few do even now.

Communication between data subjects could change over time to help secure our privacy for the years to come. However, it's yet to be seen how that will impact fraud in the long term, as we may have increasingly limited access to consumer data.

Simon Fogg, data privacy expert and legal analyst, Termly.io

U.S. companies are now considerably more cautious when targeting customers in the EU. Even though the GDPR came into effect over a year ago, over 1,000 major US publications are still unavailable to EU users — either because those publications never finalized their compliance efforts or because they felt their European customer base wasn't large enough to justify the necessary (and costly) changes. U.S. companies used to cast a wide net in their data collection practices, but the GDPR has forced many to navigate data boundaries with increased vigilance.

We should expect the number of fines levied for GDPR noncompliance to skyrocket. Although few notable penalties have been issued so far, regulators are still dealing with a large backlog of data breaches. Once they catch up, they will begin to wield their authority with greater force, and companies in the U.S. are likely to be among those hit.

Sweeney Williams, vice president of security, privacy & compliance, Vision Critical

Prior to GDPR, U.S. companies with no physical presence in Europe could operate with little or no regard to EU privacy requirements, since the reach of enforcement was limited and potential fines were low. The GDPR has forced U.S. companies not only to take notice of EU requirements, but to actively enact and enforce those requirements in their own operations, often at great expense. Thousands of companies have hired data protection officers, created complex data flow maps, implemented data subject access processes across dozens of disconnected applications, and made significant upgrades to their data security and privacy operations. On the other hand, a number of U.S.-based companies have chosen to shut down operations that were either located in the EU or were providing products and services to the EU, believing that the cost of lost revenue would be lower than the cost of compliance and potential fines. Some have even gone so far as to block European IPs from connecting to their websites.

The single most significant and beneficial impact of GDPR, both within and outside of the U.S., has been its influence on the public, due to the strong data subject access and transparency rights it features. While the underlying concepts contained in GDPR are not new, awareness of data privacy rights has skyrocketed as a result of the unprecedented amount of press the regulation has generated since its introduction. Individuals now expect to receive the same level of transparency, data access and control rights as those contained in GDPR, and regulators around the world are facing significant pressure from their constituents to enact GDPR-like data privacy legislation in their own countries. In the U.S. specifically, the rate of newly proposed data privacy regulations is at an all-time high and is likely to culminate in the creation of the first-ever U.S. federal privacy law.

Aki Estrella, privacy advisor, Stellae Legal and Risk Advisors

Mostly, GDPR has changed how companies deal with information and the way they plan for its use. Segregating information, sending notices and training employees/departments to respond to requests from EU citizens have been the most ordinary impacts; however, as we've seen, a few companies haven't quite gotten things right and are dealing with the staggering fines associated with the GDPR. I don't see any scale-back of companies using data or selling to the EU.

Extra Security

Intellectual property theft: What it is and how to defend against It

Ilia Sotnikov

VP of Product Management at Netwrix,
Official member of **Forbes Technology Council**

Many businesses rely on innovation and knowledge to beat the competition and achieve success. Their intellectual property (IP) is often their most valuable asset, and they consider it to be highly sensitive information. There are different types of intellectual property; they include copyrights, trademarks, patents and trade secrets. Some IP is protected under the terms of state and federal intellectual property laws; examples can include innovations, advances in technology, formulas, business processes, media products, web content and music. Because IP protection is a very complicated area, companies often seek the services of intellectual property attorneys, who help them respond to instances of trademark, patent or copyright infringement.

Intellectual property theft occurs when a person steals these assets. Potential outcomes like economic damage, the loss of a competitive edge and slowdown in business growth define intellectual property theft as a serious concern for businesses. According to the Update to the IP Commission Report released in 2017, the U.S. economy loses over $225 billion annually due to IP theft in categories such as counterfeit and pirated tangible goods, patent infringement, and pirated software.

The media often talks about global enterprises falling victims to IP theft while similar stories about small companies go unreported. The truth is, the risk of IP theft is high for companies of any size. In fact, the 2018 Netwrix IT Risks Report found that SMBs are even more vulnerable to IP theft and cyber espionage than enterprises. These cases just don't get as much attention.

Let's take a closer look at the 2018 Netwrix IT Risks survey responses to learn about the most frequent intellectual property theft scenarios and the security practices that help with intellectual property protection.

What are the most common IP theft scenarios?

Human errors. 51% of survey respondents named human errors as a common method for intellectual property rights infringement. This happens when employees lose devices, accidentally send files containing trade secrets outside the company network, or fail to uphold their responsibility to not share confidential data with unauthorized parties. For example, in October 2017, an Apple engineer brought his daughter to work — where she filmed the unreleased iPhone X for her vlog. The footage included an iPhone X with special employee-only QR codes and a notes app with the code names of unreleased Apple products.

Malware infiltrations. 48% of survey respondents have suffered malware infiltrations. Malicious software enables criminals to steal an enormous amount of IP. For example, from around 2006 to 2018, a hacking group called Advanced Persistent Threat 10 (APT 10) targeted the networks of more than 45 technology companies and U.S. government agencies in order to steal information and data concerning a number of technologies. In addition, the hackers attacked the computers of managed service providers (MSPs) and accessed the networks of their clients. By using spear phishing techniques to introduce malware onto computers, they were able to steal of hundreds of gigabytes of intellectual property and other confidential business and technological information.

Privilege abuse. The third most common root cause of IP theft, according to the Netwrix research, was privilege abuse, which was named by 34% of respondents. By exploiting their access to sensitive files, employees commit economic espionage and steal trade secrets. An unfortunate tale which happened at biotechnology company GlaxoSmithKline (GSK) serves as a good illustration. A group of conspirators, including a former GSK research scientist, stole trade secrets to benefit a Chinese pharmaceutical company. According to the U.S. Attorney in the case, the GSK scientist emailed confidential files and transferred portable electronic storage devices containing trade secrets to his China-based associates. In 2018, two of the defendants pleaded guilty to intellectual property theft, but the exact amount of financial damage has yet to be calculated.

Who is responsible for IP theft?

A strong defense against IP theft must involve measures against not just outside attackers, but insiders as well. Even if an attack is initiated from the outside, it is often an employee who disregards privacy policy and clicks on a malicious link that lets the attacker into the network. Insiders also copy sensitive data from their work computers to USB drives and then lose them, putting the data in the hands of outsiders. Unfortunately, the report shows that 29% of companies are still sure that hackers are the most dangerous threat actors when it comes to IP theft, while over 60% of the incidents they experienced were actually caused by regular business users. IT staff, who are perceived as the least dangerous threat actor, were responsible for 30% of reported incidents.

Departing or terminated employees also require attention. Take a look at these figures: Only 25% of companies think that these employees are an important risk factor, but 39% named them as the threat actors responsible for actual security incidents.

What do companies do to protect against IP theft?

The survey reveals that organizations are not doing enough to protect themselves against IP theft. It's not only that they underestimate the risks coming from their own employees; they also fail to implement security basics. 36% of organizations conduct asset inventory once a year or less frequently, 20% almost never get rid of stale and unnecessary data, and 17% have never performed IT risk assessment.

Moreover, the survey results show that 44% of companies still don't know or are unsure about what their employees are doing with sensitive data. With this lack of visibility, it's almost impossible to detect cases of intellectual piracy in a timely manner.

Only 19% of companies classify data once a quarter. Moreover, even though data access rights should be updated every 6 months to help prevent inappropriate access, 51% of organizations perform such checks less than once a year.

How can organizations minimize the risk of IP theft?

To better protect against intellectual property theft, companies say they want to improve detection of security events (68%) and implement security safeguards (63%).

We also recommend the following best practices:

- **Gain visibility into sensitive data.** Knowing exactly what sensitive data you have and who has access to is the initial step in building strong security posture. Using an automated data classification solution will help you dealing with the loads of data being created or modified daily.
- **Establish a data security policy.** A security policy defines how security threats are addressed, specifies which controls are needed to mitigate IT security vulnerabilities, and defines a recovery plan should a network intrusion occur. Your security policy must be verified by your legal department and signed by your CEO. The document should contain what actions will be taken and what penalties will be applied if these policies are violated and your investigation identifies the culprit.

- **Monitor employee activity.** Even if you trust those who have access to your sensitive data, they are still are the biggest threat, because even people without bad intentions can make critical mistakes. That's why it is important to establish user behavior monitoring. Pay particular attention to abnormal spikes in activity, which are a sign that something could be wrong.
- **Involve HR.** It's a good idea to coordinate with HR and be notified whenever an employee is leaving so you can watch for suspicious activity, such as bulk file copying, before they leave and disable their accounts promptly when they are gone.
- **Provide training to employees.** Poor cybersecurity awareness of employees increases the risk of IP loss. We recommend establishing training programs for employees based on their roles and the level of access they have in your network. Explain what a potential attack (such as phishing) looks like, how it works and what the consequences are. Remind everyone about your password policies and encourage employees to report security incidents. Work to avoid misunderstandings; your IT department should be open to questions and concerns from regular users regarding your security program.

Intellectual property helps drive a company's competitiveness and growth, so trademark, patent, trade secret and copyright protection should be an integral part of every security strategy. Building a strong line of defense requires a company-wide involvement, from regular users to top executives. Knowing that risks are rising, companies should ensure they have proper security policies around sensitive data protection and continue working with their employees to minimize risks coming from insiders.

Extra Security

Cloud data security: 4 questions to answer before moving your data

Earl Follis
Technology Evangelist and Consultant

Cloud service providers are constantly improving their offerings in order to provide a stable, secure, cost-effective platform on which almost all IT applications can run. For example, they often support multiple virtualized operating systems, customizable server processor counts, flexible network configurations and other cloud storage parameters. And to help ensure cloud data security, vendors offer functionality like access control, key management and encrypted data.

Still, moving data and applications to the cloud has wide-ranging implications for your organization. In this blog, we'll explore several key questions that you should consider thoroughly before you bet your company's future on a cloud environment.

What are the main benefits of moving data to the cloud?

Migration of applications and data to the cloud has been a boon to IT shops of all sizes around the world. The convenience of anytime, anywhere data availability and the potential cost savings alone make it a compelling alternative to traditional data center-based physical infrastructure. But there are many other benefits as well.

One is data redundancy — cloud data is typically replicated among more than one geographical zone. Most public cloud services even allow customers to specify which geo-zones their applications and data reside in. Although this replication does not constitute a comprehensive data protection or data security plan, it does offer peace of mind that multiple copies of your data reside in the cloud environment.

Moving data to the cloud can also help companies meet security and compliance requirements that focus on data availability, data redundancy and information security. It's not that cloud-based computing is inherently more secure and robust than on-premises computing, but rather that it can increase the control IT has over company data. In particular, moving to the cloud can reduce shadow IT and get data stores out from under desks and in storage closets so they can be governed and protected in compliance with governance regulations and best practices.

How can I preserve information integrity in the cloud?

Data protection involves three critical components: data integrity, data confidentiality and data privacy. Data integrity involves ensuring that all data stored in the cloud is accurate, i.e., that the bits and bytes that you store in the cloud remain exactly as they were when they were first uploaded or created in the cloud.

There are a variety of methodologies that help ensure the data integrity of cloud storage, including provable data possession (PDP) and high-availability and integrity layer (HAIL). These techniques attempt to eliminate data loss due to intentional or accidental data manipulation, deletion or corruption in the cloud. Many cloud security solutions include data integrity management that constantly compares the current state of cloud data to the last known good data state and notifies admins of any mismatch.

How can I ensure data confidentiality in the cloud?

Public cloud computing is by its nature a shared environment — your virtual machines (VMs) are sharing infrastructure, hardware and software with other cloud tenants. As a public cloud customer, you have no idea the identity or even the number of customers with whom you share your environment. Therefore, you should closely research your cloud provider to check whether all applicable security cloud computing mechanisms are implemented and working as designed.

Private clouds offer much of the same convenience and scalability of public cloud, but do not require you to share cloud infrastructure with other customers. Probably the most high-profile private cloud in existence is the one used by the Central Intelligence Agency (CIA). The fact that an organization such as the CIA found a private cloud sufficient for their extremely sensitive requirements indicates that data security in cloud computing has matured to the point that a properly configured private cloud can meet the needs of almost any organization hesitant to trust public cloud solutions.

How can I ensure the privacy of sensitive information in the cloud?

Data privacy requires ensuring that only authorized users can access personally-identifiable information (PII), credit card numbers and other sensitive data. Many businesses have established privacy policies that control which data can be stored in the cloud and define how sensitive data is to be protected in the cloud. Cloud encryption techniques and other security measures can help prevent prying eyes from being able to access protected data. The compliance requirements applicable to your industry or company can serve as a guide to the techniques you should employ to ensure data privacy.

The high-profile data loss events constantly in the news highlight the high cost of data security issues, either on premises or in the cloud. Breaches can result in steep fines and many other expenses, particularly when the data involved is PII or other sensitive data. If you choose to store sensitive data in the cloud, you need to pay close attention to data privacy.

The stampede to cloud-based computing is not likely to abate any time soon, and neither is the growing demand for tighter requirements on data security, especially data privacy. While high-security cloud computing was perhaps a bit of an oxymoron when cloud computing was in its infancy, modern cloud services offer a variety of data integrity, confidentiality and privacy mechanisms that provide a compelling case in favor of cloud computing. Getting satisfactory answers to the questions discussed here will help IT pros find just the right fit for their cloud computing workloads.

RESEARCH

2019 Cloud Data Security Report

Learn More

Extra Security

Who is to blame for a data breach?

Ryan Brooks
Cybersecurity Expert, Netwrix Product Evangelist

The Netwrix 2018 IT Risks Report presents new research into the security threats organizations are facing and the actions they are taking to minimize IT risks. The report explores six IT risks: physical damage, intellectual property theft, data loss, data breaches, system disruptions and compliance penalties.

41% of companies named data breaches as the most critical of these risks. So, in this post, we decided to explore what companies view as the main causes of data breaches, who they think poses the biggest risk to data security and what measures they take to reduce their risk of a data breach. Here are some of the most interesting results.

Insiders, not hackers, are seen as the top threat actors

We asked our respondents who causes security incidents. Insiders took 3 of the top 4 spots in the results: regular business users (named by 51% of respondents), IT team members (35%) and departing employees (32%).

Hackers rounded out the top 4, named by 33% of IT pros. But hackers often work by trying to trick employees into opening malicious attachments in phishing emails or by taking advantage of poor corporate practices like password sharing. Therefore, regular users who fail at basic cybersecurity hygiene share responsibility for successful attacks by hackers.

Various mistakes are considered the top root cause of data breaches

We also asked about the root causes of data breaches. Human error was the top cause, named by 30% of companies. Phishing attacks were next (28%), and poor password policies (26%) took third place.

Here are a couple of stories that illustrate how each of these causes led to a real security incident:

- **Human errors: 30%**

An employee at Rainbow Babies & Children's Hospital in Cleveland, Ohio, accidentally dis-

closed private health information for about 840 patients. When sending an email to a group of patients suffering from the same medical condition, the employee put the recipients' email addresses in the To field instead of the BCC field, thereby disclosing each patient's medical information to the entire group. In response to the incident, the hospital notified the affected individuals and regulatory bodies and reeducated employees on proper procedures for handling patient privacy.

- **Phishing attacks: 28%**

Dozens of employees at Wipro, a large IT services provider in India, fell victim to a phishing campaign that enabled intruders to compromise more than 100 of the company's computer systems and use them to launch cyberattacks against customers. Evidence suggests the attack have also targeted a number of other Wipro's competitors, including Infosys and Cognizant.

The attack is still under investigation. It is not yet clear how long the attack went undetected and exactly which companies and information were compromised.

- **Poor password practices: 26%**

Citrix Systems recently announced it would regularly force all its Sharefile customers to reset their passwords. The company claimed that this new policy was not in response to an attack, but rather was designed to reduce the risk of successful "credential stuffing" — a password-guessing attack that targets people who use same passwords across different systems and websites.

However, while forcing a password reset after a security incident makes sense, requiring regular resets violates password best practices. For example, the National Institute of Standards and Technology (NIST) warns that users who are forced to constantly change their passwords tend to choose weaker passwords and update them using common transformations, such as incrementing a number in the password, that are well known to hackers. As a result, the policy tends to hurt, rather than enhance, security.

Organizations neglect security basics

Following security best practices is critical to reducing the risks of human mistakes, phishing attacks, poor password practices and other factors that lead to data breaches. However, organizations are failing to attend to security basics.

Only 20% of companies use data classification and sort out stale and unnecessary files, and less than 25% perform regular vulnerability assessments and check whether any sensitive data is available to everyone.

43% of organizations are unsure or don't know what employees do with sensitive data — which leaves them vulnerable to the risks coming from insiders.

Knowing who has access to your sensitive data, minimizing its exposure according to least privilege and monitoring use of that data are essential parts of any data-centric security approach. After all, when you lack true visibility into what is going on in your IT infrastructure, it's impossible to ensure that data access is limited to authorized personnel only and those employees deal with the data in an appropriate manner. Lack of visibility prevents you from detecting security incidents in their early stages and responding promptly, which makes data breaches more likely.

Organizations are ill-prepared to respond to a security incident

Security best practices are not limited to strategies for reducing the risk of a successful attack. Organizations are advised to take an assume-breach posture, which involves ensuring they can:

- Quickly detect a data breach
- Respond to an incident in a timely manner
- Determine the scope of a breach
- Recover data, systems and services that were stolen or destroyed

However, the Netwrix report shows that only 17% of organizations have an incident response plan, provide training for employees and conduct test runs. 19% have an approved plan but never followed through on the other steps, and 26% have only a draft of a plan. This puts them at increased risk of missing a breach or handling it improperly, which can dramatically extend the impact of an incident — companies are justly criticized for being slow to inform customers when their personal data is compromised, and regulators hike compliance fines when data breach reporting requirements are not met.

Building a strong cybersecurity posture has never been an easy task, and the increasing complexity of both IT environments and the threat landscape makes it harder than ever. The good news is that companies are increasingly ready to commit to allocate budget to cybersecurity — respondents report that their cybersecurity investments grew by 117% in the past 3 years and they expect them to increase by 143% over the next 5 years. For most organizations, focusing that additional budget on security basics and implementing best practices will deliver the most value.

WHO IS TO BLAME FOR A DATA BREACH?

netwrix

TOP 3 THREAT ACTORS

51% Regular business users

35% IT team members

32% Departing and terminated employees

TOP 3 DATA BREACH ROOT CAUSES

30% Human errors

28% Phishing attack

26% Poor password practices

FEW ORGANIZATIONS IMPLEMENT SECURITY BASICS

20% classify their data and get rid of stale and unnecessary files

12% perform regular vulnerability assessments

10% check whether any sensitive data is available to everyone

43% of organizations are unsure or don't know what employees do with sensitive data

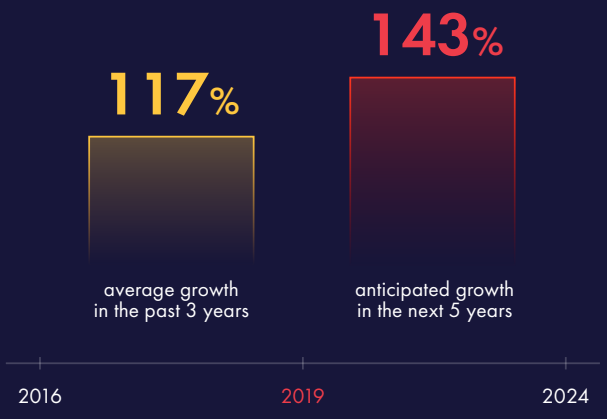
FEW ORGANIZATIONS TAKE INCIDENT RESPONSE SERIOUSLY

17% have a plan, provide training for employees and conduct test runs

19% have an approved plan but no enforcement

26% have just a draft of a plan

CYBERSECURITY INVESTMENTS: TODAY AND TOMORROW



CYBERSECURITY AREAS TO IMPROVE*

69% Protect

61% Detect

56% Identify

39% Respond

31% Recover

* based on NIST Cybersecurity Framework

First-Hand Experience

Horizon Leisure Centres accelerates data classification to comply with GDPR & saves £80,000

The GDPR is a tough regulation, especially for companies with limited financial and human resources. The costs of achieving compliance are high, but the price of non-compliance can be even higher — fines from supervisory authorities in the EU can reach 20 million euros or 4% of a company's annual global revenues, whichever is greater.

Therefore, it's essential to discover and classify data regulated by the GDPR. Consider the case of Horizon Leisure Centres, a UK-based not-for-profit organization. It stores personal information about its members, such as medical information and driver's license data, across 500,000+ folders and subfolders. To comply with the GDPR, the IT team must secure this information and make sure they can quickly satisfy requests from data subjects (processing restrictions, erasures, etc.). Otherwise, Horizon would be subject to additional and more thorough checks by the UK's Information Commissioner's Office (ICO) and heavy fines that could lead to complete closure of its centers.

But the costs of performing these tasks manually are often prohibitive. Iain Sanders, IT Manager at Horizon, notes that "finding all data we store on a single person would take around two weeks of manual work by four IT specialists. With more requests, discovery could take them the whole month, so we would have to expand the IT team and hire four additional employees, paying them up to £80,000 per year in total. As a non-profit, we cannot afford this."

Finding the solution

Horizon Leisure Centres started looking for ways to gain better visibility into its data 15 months before the GDPR came into effect. They realized that automated data discovery and classification would help them see exactly what kinds of data they have and where it is located so they could secure it in accordance with GDPR requirements and uphold data subject rights.

Now, with automated data discovery and classification in place, they can easily identify all files containing regulated information so they can ensure they are in secure locations and only proper personnel have access to them. Moreover, with all their data across half a million folders properly classified and tagged, they can retrieve all information required to satisfy a data subject request by simply searching for the customer's name or other identifying data. The process takes one person just a few minutes — a huge savings over the two weeks of manual work by four employees that would have been required for each request without data classification.

Moreover, the automated data discovery and classification solution helped Iain's team enhance the security of regulated data by improving detection of improper activity around it. Now they can easily review activity around sensitive files and folders to detect anomalous actions that might require their attention. Iain also gets alerts on suspicious events, such as the bulk modification, deletion or copying of data and excessive failed access attempts, so he can respond promptly to threats to regulated data.

With the GDPR in effect, protecting data privacy can be considered a basic cost of doing business. Achieving compliance isn't simple or cheap, but it can be far less expensive than the penalties for non-compliance. One key way to control the costs is to invest in the right security solution, one that streamlines the process of data discovery and compliance.

Read more stories like this on
www.netwrix.com/go/success_stories

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides.

Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

For more information visit www.netwrix.com

Corporate Headquarters: 300 Spectrum Center Drive, Suite 200 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

EMEA: +44 (0) 203-318-02