WHY DATA BREACHES SHOULD CONCERN YOU WHEN IT COMES TO GDPR
DATA BREACHES CONTINUE TO GROW IN VOLUME AND SCOPE

In today’s business community, data breaches are an epidemic. They infect organizations of all sizes, in every nook and cranny of the world. Globally, cyber-crime damages are expected to double by 2021, totaling $6 trillion.¹

The perpetrators of these attacks are generally after individuals’ personal data such as names, birthdates, and financial or medical information. They may build a Trojan horse that installs malware when a user clicks a seemingly innocuous email attachment, or they may set loose a virus or worm that propagates itself from system to system. Once a network is infected, the malware may seek out sensitive information, or it may record user keystrokes needed to access the desired data.

PERSONALLY IDENTIFIABLE INFORMATION AT RISK

Cyber attackers are looking to steal personal information in bulk, with the goal of monetizing it. They may simply sell it on the dark web, or they may hold the data hostage, threatening to sell it if they don’t receive a ransom. They may use stolen financial information themselves to hack bank accounts, make purchases on stolen credit cards, etc. Or they may use the data to perpetrate other crimes—for example, consolidating health and personal information to create patient profiles that can be used in insurance fraud schemes.

Hackers can be incredibly creative in accessing personal information. One recent attack involves a worm that spreads via Bluetooth, actively searching for vulnerable hosts.² Another impersonates Flash player update tools or similar applications. Once installed by an unwitting mobile phone user, it then presents a fake bank web page to capture the user’s login credentials.³
TALLYING THE COST OF DATA BREACHES

All of this translates into an environment where data breaches are becoming commonplace. Ponemon Institute’s “2017 Cost of Data Breach Study” projects that companies around the world face a 27.7 percent chance of experiencing a material data breach over the next two years. The organization defines a “material” breach as one in which 1,000 or more records containing personal information are lost or stolen. This is an increase over last year, when Ponemon estimated the average probability of a data breach in the following 24 months was 25.6 percent.⁴

For companies that are victims, breaches are painful. Ponemon estimates that the average cost of a data breach is $3.62 million, or $141 per lost or stolen record.⁵ Companies that lose crucial customer data may face legal action, with the prospect of judgment or settlement amounts in the millions of dollars.⁶

Long-term damage to the organization’s brand may be even more debilitating. Companies may receive negative press for years, and that can significantly affect revenue. Research shows that consumers are less trusting of companies that have suffered a major breach. Seventy-six percent of respondents to a recent consumer survey said they would move away from a company that experienced too many such incidents.⁷

Likewise, individuals with IT security responsibility may find their personal brand damaged in a security breach. Major breaches often lead to resignations of IT security directors, CIOs, and even CEOs.
IMPLICATIONS OF GDPR FOR DATA-BREACH RESPONSE

Anyone with responsibility for organizational security has an obvious incentive to avoid a high-profile incident. The European Union (EU) is now upping the ante by deploying far-reaching regulations that give companies further incentive to improve data protection. Any organization that does business in the EU—or that otherwise touches identifying information on EU residents—faces consequences if it fails to comply with the upcoming General Data Protection Regulation (GDPR).

Scheduled to take effect on May 25, 2018, GDPR regulates how companies collect, process, handle, and/or store the personal data of any resident of the EU. GDPR defines “personal data” as information about an individual that could be used to directly or indirectly identify him or her. It can include anything from a name, photo, or biometric information to financial data such as bank account information. Contact information such as an email address would also qualify, as would social media posts and a computer’s IP address or cookie records. Further personal data might include medical and genetic information, political opinions, sexual orientation, and racial or ethnic information.

And here’s the kicker: Companies do not need to have any type of operational presence in the EU to fall under the GDPR umbrella. **Every company that touches personal information of EU residents falls under the regulation.**
GDPR NOTIFICATION REQUIREMENTS

One of the new mandates under GDPR is that a breach of such personal data must be reported to the appropriate supervisory authority within 72 hours, where feasible, if the incident is likely “to result in a risk to the rights and freedoms of natural persons.”

An individual’s rights and freedoms would be at risk if, for example, possible outcomes of a data breach might include discrimination against the person whose data was stolen or damage to that individual’s reputation. Other qualifying scenarios might involve financial loss to the individual or loss of confidentiality that should be assured, such as with medical records. In the event of a data breach that meets these criteria, the company must notify the appropriate authority in a way that:

- Describes the nature of the breach, including the number of individuals affected and the number of personal data records involved;
- Describes the likely consequences of the breach; and
- Describes measures taken or proposed to mitigate any possible adverse effects of the breach.

When a breach poses a “high” risk to the rights and freedoms of natural persons, the notification requirement doesn’t end with this report to the regulator. In that case, the controller of the data—that is, the organization that collected the information—“shall communicate the personal data breach to the data subject without undue delay. [This] communication…shall describe in clear and plain language the nature of the personal data breach.”

IMPLICATIONS FOR CORPORATE DATA SECURITY

In a significant departure from existing data protection regulations, GDPR imposes substantial penalties for noncompliance. The regulation includes two tiers of maximum fines depending upon the severity of the noncompliance: 10 million euros or 2 percent of an organization’s global revenue or 20 million euros or 4 percent of an organization’s global revenue. In either case, the fine will be the greater of the two. For all violations, actions taken by the company to mitigate the damage of the data breach will be taken into consideration as fines are assessed.

The financial repercussions of a data breach could be even greater than the potential fines suggest. In addition to the penalties imposed by regulatory authorities, anyone whose personal data is stolen may seek monetary damages from the company that collected the data and from any other business that has been involved in processing it.
**BEHIND ON READINESS**

In July 2017, a mere 10 months before the GDPR rules take effect, Information Age reported on a study that showed only 40 percent of companies in the U.K. had begun to prepare for the new regulatory regime, as had 28 percent of businesses in the rest of the EU. At that time, only 5 percent of companies in the U.S. had started preparations.  

Even worse, only 9 percent of U.S. IT professionals in the study said they considered themselves informed about GDPR and its possible impact on organizations. Despite this single-digit knowledge of GDPR, a full 43 percent of U.S.-based respondents claimed that GDPR would not affect their organization at all.  

Every company that interacts with the “personal data” of EU residents at any juncture in their operational processes will have to comply. Gartner predicts that by the end of 2018, more than half of organizations affected by GDPR will not be in full compliance with its requirements.  

To be compliant with the regulation when it takes effect, businesses ought to be shoring up their processes right now. They need to understand why they’re collecting data and what types of data they are collecting and storing. For all personally identifiable information, they need to know the nationality of the individual, where the data is stored, how and when it is communicated, and what security measures are in place to protect it.  

The U.K. Information Commissioner’s Office warns: “You should put procedures in place to effectively detect, report, and investigate a ‘personal data’ breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the [proper supervisory authority] or affected individuals if a breach occurred. Larger organizations will need to develop policies and procedures for managing data breaches.”  

**GDPR COMPLIANCE MAY REQUIRE BUSINESS PROCESSES TO CHANGE**

As GDPR’s effective date looms ever larger, IT security directors need to increase their visibility into every instance of corporate data. They need to understand how the information is used, for what purpose, and by whom.  

These insights are helpful in any case, but they will be crucial if the organization ever faces a GDPR data-breach reporting deadline. A company staring down a three-day timeline for researching, responding to, and then reporting on a data breach has no time to waste searching for information or determining which data is impacted by GDPR and which isn’t. Globally, the average time to identify a data breach is 191 days, and the average time to contain it is another 66 days.  

With the GDPR effective date looming, IT security directors need to be focusing attention on shrinking time to detection and mitigation. At present, the divide between reality and what is mandated in GDPR is huge.  

“GDPR compliance will require changes to some core business processes, including data processing workflows, organizational structures, and even core business policies,” says Drew Del Matto, CFO of Fortinet. “The process is going to require taking a fresh look at existing security solutions and strategies. Network security will not only need to actively prevent intrusions, [but] it will also need to minimize the risk of serious breaches by reducing the time it takes to detect and respond to new threats.”
ADDRESSING “SHADOW IT” AND CLOUD-BASED SYSTEMS

In many organizations, building visibility into the data life cycle may require IT security directors to address the security implications of employees’ “shadow IT” systems. These are solutions that exist outside the officially sanctioned corporate infrastructure, but that employees nevertheless use for company business. Some organizations may find that employees are even sharing GDPR-affected data via online public cloud applications such as Dropbox or Google Drive.

Transmitting data through these types of third-party applications does not absolve a company, or its staff, from the rigorous security and notification requirements of GDPR. The organization that collected the data, as well as the organization whose employees continue to store and handle it (if they’re different entities), is still beholden to GDPR data protection rules, regardless of what type of software the data is traveling through.

The complexity of data-breach notifications rises exponentially when users take information outside established corporate channels. The burgeoning number of devices that are part of the Internet of Things (IoT) further complicates compliance. Nevertheless, the company’s responsibilities to supervisory authorities, and to the individuals whose data it is handling, remain the same—regardless of whether data is stored locally on-premises or on a public, private, or hybrid cloud.

IMMUNIZE YOUR IT SECURITY STRUCTURES

Data breaches are inevitable. Every company’s systems will be infected from time to time, regardless of the breadth and number of intrusion-prevention solutions and processes that it deploys. As the frequency of incidents continues to increase, the key to maintaining healthy IT security practices, and avoiding a plague of bad PR, will be to ensure that systems and processes are ready to enable rapid detection and effective post-intrusion response.

GDPR dramatically compresses timelines from initial threat detection to remediation. It’s incumbent on IT security directors to build an infrastructure that shrinks the window for breach detection and mitigation, and to do so before GDPR takes effect.

The company’s responsibilities remain the same, regardless of whether data is stored locally on-premises or on a public, private, or hybrid cloud.

FIRST STEPS IN GDPR PREPARATION

1. Engage a third-party firm to conduct an assessment of your data protection practices and exposure to GDPR rules.

2. Understand what personal data you collect, or handle in any way, and whose data it is.

3. Determine where any GDPR-impacted data is stored, as well as how it is communicated between systems and to cloud environments.

4. Estimate how long data-breach detection and mitigation currently take your organization so that you have a sense of where you stand vis-à-vis data-breach requirements in GDPR.
WHITE PAPER: WHY DATA BREACHES SHOULD CONCERN YOU WHEN IT COMES TO GDPR

5 Ponemon Institute. "2017 Cost of Data Breach Study."
8 EUGDPR.org.
11 General Data Protection Regulation, Article 33: “Notification of a personal data breach to the supervisory authority.”
12 General Data Protection Regulation, Article 34: “Communication of a personal data breach to the data subject.”
13 General Data Protection Regulation, Article 83: “General conditions for imposing administrative fines.”
14 Nick Ismail. "Who is more prepared for GDPR? The UK, Europe or the US?" Information Age, June 27, 2017.
15 Nick Ismail. "Who is more prepared for GDPR? The UK, Europe or the US?" Information Age, June 27, 2017.

Copyright © 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.