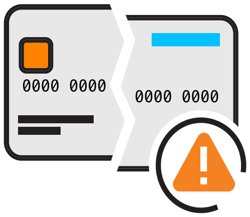
The Hidden Costs of Data Breaches

Why your company's reputation and bottom line are at stake



Data Breaches by the Numbers:

- **$3.6 million**—Average cost of a breach
- **$141**—Average cost of each record breached
- **214**—Average number of days to detect a breach
- **77**—Average number of days to respond to a breach

Source: Ponemon Institute's "2017 Cost of a Data Breach" study

Year after year, cyberattacks grow more sophisticated, more pernicious, and more prevalent. And with advanced cyberweaponry finding its way into the hands of the common cybercriminal, organizations of every size risk being attacked. So, today's companies need to understand what the consequences will be when it happens.

✓ What's the Bottom Line?

You know what they say: If you have to ask, How much? You probably can't afford it.

That saying holds true for most companies. Unless $3.6 million is something they can afford. That's the figure that the Ponemon Institute cites as the average cost of a data breach in its 2017 Cost of a Data Breach Study. What's more, every single record breached costs a company an average of $141.00. For organizations storing and managing sensitive data records numbering in the tens of thousands or more, that's a lot to lose. These records could include medical, personal, or financial information, and map to a variety of industries such as healthcare, financial services and insurance, retail, legal, public administration, and more.

In reality, however, the costs from a data breach span an enormous range depending on a company's ability or lack thereof to detect when data is being exfiltrated or destroyed, as well as its response once that's determined. That can mean the difference between thousands of records becoming compromised or merely hundreds–which gives companies with effective detection and response strategies an upper hand once a breach occurs.

✓ Like Cyberthreats, the True Costs Can Be Hard to Detect

Some costs of a breach are immediately evident, such as the detection and escalation costs associated with the salaries and fees of the security teams required to perform investigations and forensics, the costs for public notification via public relations and press announcements, post-data breach response costs related to hiring an incident response team, and any necessary or required communications through phone calls and emails to those who need to know or might be affected. Depending on the circumstances, legal fees and regulatory fines and compliance penalties may become part of the equation too.

Yet tallying the blow to company finances isn't always clear at first. Business disruption can be hard to quantify. It may involve volatility in stock prices, a spike in the customer churn rate, increased costs to acquire new customers, and of course, severe damages to a company's reputation and brand from which it may never recover. Not to mention myriad opportunity costs, from lost business caused by service disruptions to foregoing existing plans and programs to lead–what needs to be–a swift and formidable response to mitigate damages once the breach is detected.

These costs can add up to breathtaking figures. In fact, for a few unlucky and unprepared companies they've topped more than $100 million.

✓ High-Profile Breach Examples

Equifax– (~$600 million): In the largest data breach of 2017, more than 145 million people (half of the U.S. population) had their personal information compromised. Included were names, social security numbers, birth dates, home addresses and, in certain cases, driver's license numbers. The credit reporting giant has, in part, itself to blame. The breach occurred when cybercriminals exploited a known vulnerability that the company never got around to patching.

Making matters worse, Equifax's response to the breach was wholly inadequate. In fact, it serves more as a warning of what NOT to do. Equifax failed to notify affected consumers in a timely manner, and then sent them to a new website operated by the company but not under its domain for information on opt-in ID protection services.

Merck– (~$300 million each quarter, potential to reach $1B): German pharmaceutical group Merck was victimized during the summer of 2017 to the tune of more than $300 million in quarterly losses by the NotPetya malware attack. As staggering as that amount is, NotPetya cost FedEx about the same figure in losses, and shipping giant Maersk nearly as much. As it did with these other victims, the insidious malware spread laterally across networks, encrypting machines' entire hard disks by overwriting their master reboot records. The company's manufacturing processes were affected for months. That meant Merck couldn't produce its product in bulk, driving soaring opportunity costs.

City of Atlanta– (~$3 million and rising): The costs involved in the recent SamSam ransomware attack on the City of Atlanta's vulnerable java-based servers are more in line with what companies typically face. While the city never paid any ransom, it allocated resources to a security solution for emergency incident response services, consulting services for cybersecurity crisis management, as well as public relations, among other expenses.

This attack is indicative of the fact that governments of all sizes are often vulnerable targets of cybercriminals. In Atlanta's case, beyond the damage to its budget, citizens were unable to use the municipal website for weeks. The Department of Watershed Management couldn't accept online or telephone payments for water and sewage bills, the Department of Finance no longer issued business licenses through its web page, and the Atlanta Municipal Court had to reschedule hearings and was unable to process ticket payments either online or in person. These are just some of the examples of the damages caused by the breach.

✓ Why a SOC-as-a-Service Is the Best Solution

As previously mentioned, the costs of a breach vary widely. The two greatest variables being, of course how quickly a company can detect a breach as it's happening, and then how rapid and effective the response.

In the Ponemon Institute's latest study, the average time to detection is 214 days, with another 77 days needed to contain the attack. That can give cybercriminals all the time they need to exfiltrate data and do extensive damage to an organization. It's a given then that reducing these times will significantly limit costs due to a breach.

Time and time again, the persistence of today's evolving cyberthreats prove that prevention-based security products such as endpoint AV solutions or strategies based on deploying in-house SIEMs fail to deliver on their promise to keep businesses secure. It's no longer a question of if or even when you'll be breached, but how often, and how effectively will you be able to respond. Large enterprises are able to achieve advanced levels of security by building and staffing up a 24x7 security operations center (SOC). Unfortunately, the cost of operating and staffing a fully-operational SOC is well beyond the budget of most smaller businesses, and this is where a SOC-as-a-service comes to the rescue.

With effective detection through continuous, 24/7 monitoring that includes skilled security engineers to triage and analyze alerts, as well as a response team to coordinate the necessary logistics needed to successfully contain the threat, organizations can shave weeks or months off detection and containment time. That means thousands–and, in some cases millions–of sensitive data records can be saved. Among Ponemon's findings is that companies would save approximately $1 million on average if they were able to detect a breach within 100 days and contain it within 30.

✓ Options for Small to Midsize Enterprises (SMEs)

Organizations large and small in every industry are at risk of major breach. That's why all companies need a SOC and a security team well-versed in incident response. While a realistic proposition for large enterprises, other organizations aren't so lucky.

Arctic Wolf's AWN CyberSOC™, however, offers an alternative. It is a SOC-as-a-service solution that includes the necessary security capabilities today's businesses require. To learn more, read our white paper on the subject.

ARCTIC WOLF

©2018 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

AUTHORIZED PARTNER eagle™

Eagle Technologies
www.eagleinc.com
800.477.5432
contact@eagleinc.com