If your company faced a cyber attack this year, it could cost $3.8 million. That’s according to a new study from the Ponemon Institute, a cybersecurity company based in Traverse City, Michigan. The recently released “Cost of Data Breach Study: Global Analysis,” sponsored by IBM, found that cyber attacks are also increasing in frequency.

“The bad guys are very sophisticated, and when they detect a vulnerability, they’ll take advantage of it,” says Larry Ponemon, chairman and founder of the Ponemon Institute. “If you don’t have the right structure in place from a security perspective, you could be dealing with a big problem.”

The Ponemon Institute examined the records of more than 350 organizations worldwide that experienced data breaches—meaning sensitive, protected or confidential data was lost or stolen and put at risk.

The study includes research from more than 1,500 interviews with IT, compliance and information security professionals in 11 countries. Cost figures were determined using field-based research methods and activity-based costing, which added direct and indirect costs related to the violations, Ponemon says.

**The High Cost of Cyber Attacks**

According to the study, the cost of dealing with breaches has increased 23 percent in just two years. The most expensive breaches occurred in the United States, with an average of $217 per compromised record. Germany was second most expensive at $211 per record.

The direct numbers include the expense of hiring forensic experts to determine what happened in the breach and how much data was compromised, Ponemon says. But indirect costs can also affect a company, such as the expense of creating response teams of employees who may have to spend their workdays and weekends dealing with the breach. Additionally, a meltdown of trust between companies and their customers causes opportunity losses.

Companies in more regulated industries tend to experience
higher costs for security problems. “If you’re a bank, having a breach means you’re out of compliance,” Ponemon says. So in addition to resolving the breach, there also could be costs related to regulatory penalties. “It takes more effort to recover,” he says.

Other industries with higher-than-average costs for security breaches are healthcare, pharmaceutical and telecom. Healthcare companies had the highest cost per stolen record, with an average of $363, according to the study.

These types of industries also tend to face a higher reputation cost in a security breach. “Most people believe their bank or healthcare provider is taking serious steps to protect their data, and the expectations are really high,” Ponemon says. So a security loss results in greater disappointment with the company.

Another factor in the increased price of data breaches is that the general public is more likely to pay attention to security failures now than in the past. Five or six years ago, if someone received a letter from their bank saying their records had been exposed, the customer may have been concerned, but unsure how it would affect them personally. But as data breaches occur more often, they’re getting more media coverage. Recent news stories have highlighted hacks involving movie studio emails, unauthorized logins and access to healthcare company records. As a result, the average consumer is paying more attention.

Many people are responding by taking proactive steps such as buying monitoring plans to check their credit records or freezing their credit altogether, Ponemon says. And they may stop frequenting businesses that have security breaches.

Not only could that cause loss of income, but businesses with a spotty reputation for protecting information may have a harder time earning new customers, which would likely increase their customer acquisition costs. It’s crucial for companies to know how to identify and block potential security breaches.

Understanding Hacker Motivation

Malicious or criminal attacks were responsible for 47 percent of all breaches, and they also were costlier than breaches caused by other reasons, such as technology glitches or human error, according to the study. When it comes to malicious attacks, generally four categories of hackers exist:

- **Criminal syndicates.** These organized groups

Jos Svendsen
PR and Communications Manager for EMEA, Milestone Systems

Prior to joining Milestone Systems, Jos was online business developer with Carlsberg and online marketing manager and partner communications manager for Microsoft. He was also a journalist for PC World and editor-in-chief for Computerworld.
tend to have sophisticated operations and are financially motivated. They plan to monetize security attacks on companies by selling stolen records or conducting similar acts of criminal behavior.

- **State-sponsored attackers.** Similar to criminal groups, these hackers often operate with the support of a government.
- **“Hacktivists.”** These are hackers who breach a company’s data to advance an activist cause. “They don’t do it to monetize; they do it to make a point. They’ll try to embarrass the company by exposing confidential information, such as exposing a company’s human resources records,” Ponemon says.
- **Lone wolf.** A person who’s acting alone and may view hacking into a company’s data as a challenge. It’s someone who wants to get into a system just because it’s there—they find it interesting or want to get away with it.

### Unintentional Breaches Are Also Costly

Though criminals are responsible for a large portion of data breaches, problems can also be caused by technology malfunctions and human error.

Risky practices that employees engage in can include connecting company computers to unsecure wireless networks, sharing passwords with others and leaving computers unattended while outside of a secure worksite. “Good people make mistakes,” Ponemon remarks. But as a result, an unintentional data breach could cost a company millions.

On a positive note, it may take less time to recognize unintentional security breaches and take steps to stop them. According to the study, it took 158 days on average to identify human error breaches, while malicious attacks were discovered after an average of 256 days.

### Implementing the Right Security Measures

A company can protect its systems in many ways. While no measure is foolproof all of the time, Ponemon says taking these steps could help a company prevent—or at least quickly respond to—cyber attacks:

- **Educate employees about security protocols.** Put policies in place that call for regularly changing passwords and implement robust authentication to help prevent unauthorized access to company computers. Once companywide security processes are in place, regularly communicate them to employees.
- **Establish governance processes.** Set up command and control responsibility within the company for security and infrastructure, and task someone with addressing any problems that come up in real time. Appointing a strong leader who can set an agenda and has high reporting authority is important.

“A person who reports to the CEO, COO or CIO can make it easier to have a stronger governance process and educate people in the organization,” Ponemon says.

---

**Credit Card Security on the Midrange: The New Reality**

If you accept payments by any form of credit cards, you are probably terrified. The year it likely began for you was 2014: eBay, JP Morgan Chase, Home Depot, Community Health, Michaels. Five data breaches; 285 million affected.

It’s accelerating as more countries condone cyber crime, malware effectiveness skyrockets and merchants embrace universal electronic payment.

So businesses must find ways of getting paid more securely and efficiently, and with tighter integration to order entry and A/R systems. Companies doing call center and e-commerce operations based on IBM i are both blessed and challenged by all of this. We attract less publicity and have fewer threats to face. Conversely, we envy the cost-effective, off-the-shelf security solutions available to the Windows®, AIX® and Linux® crowd.

Advances by software vendors and service providers are providing new, more effective defenses. Remote tokenization stands as the best way to get an enterprise “out-of-scope.” However, we may sacrifice flexibility and functionality for security.

We need all three. Today’s challenge is to combine them all. We on the IBM midrange will find this our biggest project.

---

**Ira Chandler, CTO, Curbsstone Corporation**

Author of the first commercial AS/400 credit card software in 1993, Ira and Curbstone focus on IBM i payments security.
Bad guys will reinvent themselves over and over again, so what may work today for cybersecurity may not work tomorrow."

—Larry Ponemon, chairman and founder, Ponemon Institute

As part of those procedures, organizations should be ready to respond quickly to crises. “The security problems you learn about today are going to be the problems you’ll want to deal with today, so having a process in place is important to building a fast, effective incident response team,” he adds.

- **Stay up-to-date on technology tools.** You’ll want to have appropriate firewalls, intrusion prevention and intrusion detection technology, which can give you information about your system and network.

  Using advanced analytics and sharing intelligence data across your industry can also help you spot network anomalies and identify potential attacks on company systems. Having robust technology tools could also help minimize the risk of security breaches due to technology malfunctions.

  It’s also important for companies to build a strong infrastructure in other areas, such as power systems. “The bad guys hacking into systems aren’t just looking to steal data, they’re also looking to obfuscate data centers and cause massive downtime,” Ponemon explains.

  “People may not think power systems are a part of security, but if they fail, you’ve got a big problem.”

- **Regularly evaluate security strategy.** Ideally, assessing your systems should be an ongoing process, but realistically, you’ll want to comprehensively evaluate your security at least once a year, ensuring your company is implementing acceptable industry standards.

  At the same time, always look for ways to improve security. “You want to be very cognizant of how technology can change. Bad guys will reinvent themselves over and over again, so what may work today for cybersecurity may not work tomorrow,” Ponemon says. He suggests that companies also consider bringing in an objective third party to help consult on the process.

**Be Proactive**

The cost of security breaches has risen sharply in the past few years, from the tactical expenses of identifying and stopping an active breach to the indirect costs of customer loss and a harmed reputation. It’s important for organizations to be proactive in taking steps to increase the security of their systems. By having the proper governance controls, employee education and technology, companies can help make sure they’re keeping their valuable data safe and out of the hands of malicious attackers.

Margarette Burnett is a freelance writer and former IBM Jerm based in Atlanta, Georgia.

The Verdict Is In—Active Security Event Monitoring Is Critical

The security payback is huge. Active system monitoring alone can catch over 70 percent of breaches before data is lost. This is why system log monitoring with a security information and event management (SIEM) solution is in the top 10 of any list of critical security initiatives.

Why is it important to include your IBM i server in an active monitoring strategy? Because that’s where the sensitive data is! Payroll, HR, ERP, CRM and other applications all store sensitive data on our IBM i servers. For SIEM solutions to work correctly, they have to see anomalies and patterns in the events from all of your IBM i servers, user PCs, application servers, network routers and security devices in real time. In addition to security events, add information from File Integrity Monitoring to get a full solution. To send security data to your SIEM solution, you will need IBM i event collection, data translation to the syslog standard and secure TCP or UDP communications.

With the right event collection, your IBM i will play well in your active monitoring strategy.

Patrick Townsend,
Founder & CEO, Townsend Security

Patrick is an award-winning speaker and regularly blogs on data security topics.