HEALTHCARE AND CYBERSECURITY

THE PRESSURE'S ON

by Jenny Mangelsdorf

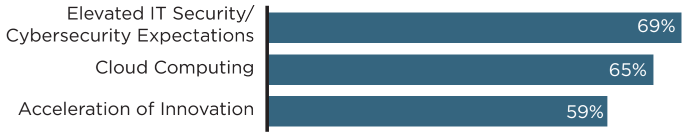
> "As attacks and threats rise, privacy and security enforcement also is rising sharply. Regulators in Australia, the United States and European Union have increased their vigilance, and a number of other governments, such as Singapore, have or will soon have new privacy laws."
>
> — Richard Staynings, CSC Global Coordinator, Healthcare Cybersecurity

As major security breaches continue to top the news, governments and organizations respond with new regulations, increased oversight and stiffer penalties. Simultaneously, increased demand for mobility and expanding supply chains, along with a desire to link IT systems to industrial control systems, adds to risk. Cybersecurity has taken center stage for healthcare CIOs, as evidenced by responses to CSC's 2013 *CIO Barometer* survey.

The fifth annual *CIO Barometer* represents the views of more than 680 IT managers, directors and officers working for organizations across 18 countries. For those operating in the healthcare sector, cybersecurity consistently appeared as a priority and challenge, regardless of whether the subject was innovation, management or cost.

Overall, healthcare respondents reported "elevated IT security/cybersecurity expectations" as the most significant development in their IT departments, at 69 percent, followed notably by "cloud computing," at 65 percent, and "acceleration of innovation," at 59 percent — each of which brings its own security challenges.

Healthcare: Significant Developments in IT Departments



"Most of the life sciences industry is having its intellectual property stolen left, right and center," says Richard Staynings, CSC global coordinator, Healthcare Cybersecurity. "Nation-funded cyberespionage units, for example, continue to infiltrate pharmaceutical companies in order to steal intellectual property so their nations can better compete in the global pharmaceutical space."

As the life sciences industry battles theft of intellectual property and works to better secure its supply chains, medical providers and insurers focus on securing personal healthcare information.

"Unlike life sciences organizations, which are being targeted by Asian state-sponsored cyberthieves, payers and providers are

No retailer wants to be the next poster child for cyberattacks. Yet megabreaches, such as those that affected Target and other retailers during the 2013 winter holidays, continue to succeed. Hackers are showing higher levels of innovation and expertise while inflicting damage to retail brands and bottom lines.

The good news is a lot of that pain and suffering can be avoided if retailers take steps to protect themselves and their customers. These steps include better incident planning, a more secure payment card security architecture and increased advanced-detection capabilities. By applying advances in cybersecurity, retailers can better prepare to respond, reduce their risks of payment card loss and more quickly detect threats — before an attack causes real damage.

Actions such as telling customers bland things they should do, such as to "stay alert," while budgeting for free credit reports, are no longer the best path forward. Instead, retailers need to plan ahead and make real changes now to lower potential damage from future attacks. Here are the top three steps retailers should take to protect themselves:

ONE: Plan your incident response in advance.

Even the most advanced attacks have a limited number of scenarios. That means organizations can develop an incident-response plan beforehand with a reasonable amount of assurance that the company will benefit from a faster and more complete recovery.

Many responses to past breaches and theft of payment card information could have been planned for in advance of the incidents. Areas such as technical remediation, forensic discovery, stakeholder communications and compliance notifications should be a part of every incident response plan today. Plus, when practicing response activities, organizations need to include all members of their internal and external response team.

Effective incident management starts with preparation. In many cases organizations fall short not in the security technology they have installed, but in how they handle the incident. Retailers need well-thought-out, documented decision-making plans and processes in place that they can use to efficiently respond and navigate through the consequences of an event.

As attacks change, so will regulations and other aspects of cybersecurity. Retailers have to ensure that their response plans continue to evolve and that practice drills stay current.

TWO: Add end-to-end encryption and tokenization.

Instead of waiting for more advanced chip card technology, retailers need to re-architect their payment card infrastructures now. By adding end-to-end encryption and tokenization-based security architecture enhancements, retailers can make it more difficult for criminals to steal consumer payment card data. Criminals can't steal what retailers don't have.

End-to-end encryption has a rich ecosystem of commercially available products that encrypt a payment card as the customer swipes it, right in the magnetic head of the card reader, and decrypts it only at the retailer's processing bank. Retailers then get paid, without ever having to risk losing a customer's payment card data.

Encryption can be added at the point-of-swipe in existing POS terminals, reducing the number of at-risk systems retailers have to maintain. By adding this type of encryption, retailers also lower their Payment Card Industry (PCI) audit costs, since they need not audit systems that don't have access to clear-track data.

Many payment card tokenization companies also have produced a variety of solid end-to-end tokenized encryption technologies that make it possible to better secure payment card track information, while still allowing data analytics engines to do their work. Same cards. Same POS. Same analytics. End-to-end tokenized encryption even saves resources, as systems that use this technology also need less PCI auditing each year.

THREE: Start real-time, sophisticated threat detection.

Besides adding technologies that reduce risk, retailers also need to keep a better lookout for criminals and keep a closer eye on their enterprise. Retailers should also track security alerts and events in their industries and the world at large. And they need to do this continuously.

Wielders of today's advanced persistent threats have broadened their original goals of disruption or destruction to include the theft of consumer data and intellectual property. Unfortunately, many times the affected organizations find these types of threats as much as a year after a breach begins. Faced with a cybercriminal market mature enough to have its own commercial off-the-shelf methods and toolkits, and the seemingly endless endpoint vulnerabilities that appear because of trends such as mobility, BYOB and the Internet of Things, retailers need better capabilities to help search for potential threats in real time.

By all measures, the latest POS breaches were not the result of a bunch of skimmers glued to POS terminals, but rather a full-scale, advanced and persistent threat that was able to remain undetected in retailers' systems for some time. By deploying a more secure payment card architecture and sophisticated detection capability, and by planning and practicing their incident response, retailers can improve their chances of surviving — or even warding off — the next threat. ■

TOM PATTERSON is CSC's Cybersecurity Consulting general manager.

▶ Watch the related video "When Payment Card Theft Strikes" at csc.com/card-theft.