

The Chief Security Officer in a hyper-connected world

As companies develop connected products, security becomes a critical job.



Introduction

In today's aggressively competitive, Internet-driven business world, CEOs are constantly striving for more digital innovation. As a result, many companies in a wide range of industries are now creating connected digital products. If you weren't a digital product company before, you are now.

For chief security officers (CSOs) and chief information security officers (CISOs), that has added a whole new slate of responsibilities to their portfolios. Now, in addition to overseeing network security, computer security, and in some cases physical security, these executives are also responsible for product security. Get it wrong, and the company can lose an immense amount of customer trust.

The new world of interconnected devices raises an array of questions for security executives. How can security leaders adapt to this changing world? How do you get organizational support for needed security enhancements? In some cases, companies view security investments as insurance—how do you price that? And where and how do you find the talent needed to meet these new expectations?

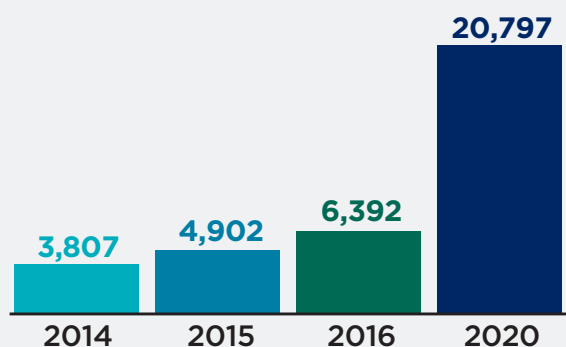
To answer these questions, Korn Ferry interviewed top CSOs and CISOs at Fortune 500 companies. Their insights show that the job, while difficult and rapidly changing, is not impossible. In short, the CSO's role is evolving and becoming more critical than ever.

New challenges of IoT devices in the business world

Connected devices are a growing part of our everyday lives. According to Gartner, in the last two years, the number of Internet-of-Things devices in the world soared nearly 70 percent to 6.4 billion in 2016 (Gartner, 2015). The research firm forecasts the IoT population will reach 20.8 billion by 2020. What this means is hackers now have more to hack. And that leaves CISOs a bigger security challenge than ever before.

Figure 1

Growth in devices connected to the internet (in millions)



Source: Gartner

The IoT attack surface

Hackers generally pose two types of threats to IoT devices. First, they can take control of a device. We've seen some frightening examples of that already. In 2015, two US researchers showed that they could remotely hack a Jeep Cherokee over the Internet, bringing the vehicle to a standstill on the highway (Greenberg, 2016). In 2016, a group of hackers took down a power grid in a region of western Ukraine to cause the first blackout from a cyber attack (Polityuk, 2016). And in 2017, an attack on Dyn, a company whose servers monitor and reroute Internet traffic, took control of hundreds of thousands of IoT devices, including printers, cameras, and even baby monitors. These types of attacks are a solemn reminder of how dependent our world is on properly functioning networks (Hilton, 2016).

Yet the second type of threat is potentially even more dangerous. Hackers can break into connected devices to get passwords and infiltrate networks. Once they get into a company's network, they can access proprietary data, customer data, and financial data, which they can leak, hold for ransom, or sell on dark markets.

Either way, the result is a hugely expensive public-relations disaster, in addition to any material damages the hack may cause.

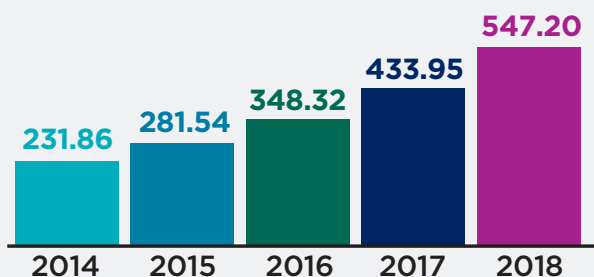
Most companies are not ready

In spite of the dangers, many companies still are not prepared for the challenges of a world in which everything from routers and printers to surveillance cameras and even manufacturing equipment presents a potential cybersecurity risk (Greenough, 2016).

Research shows many IoT devices are not properly secured. Based on a survey by analytics firm Neustar, more than 80 percent of companies that had adopted IoT were attacked in 2015. Of those, 43 percent reported theft of finances, customer data, and/or intellectual property (Neustar, 2016). In an AT&T A State of IoT Security survey only 10 percent of respondents admitted to being fully confident that their connected devices were secure, and only 12 percent were highly confident their business partners' connected devices were secure. (AT&T, 2016). The good news is, companies are slowly coming around. Investment in securing IoT devices will increase five-fold over the next five years as adoption of connected devices picks up. Gartner says security spending will reach \$547 million in 2018 and increase faster after 2020 (Gartner, 2016).

Figure 2

Global IoT spending (in millions of dollars)



Source: Gartner

Recommendations

Companies need to do more to protect themselves — and their customers. But doing so will involve organizational changes and a change in the way CSOs think about security. Here are three steps companies need to take.

1. Bring products under security

Many CSOs still think about security in terms of securing their networks, PCs, and intellectual property. But with the growth of IoT, they will need to bring their products under that umbrella, too.

Malcolm Harkins, chief security and trust officer at Cylance, a computer security company, feels companies need to adopt a more holistic view of security.

“An information risk is an information risk whether it be your infrastructure or the products you deliver to customers,” he says. “The more you have an integrated view, the better situated you are to manage those intersections.”

As part of that, senior security leaders need to broaden their thinking. “Some CSOs don’t want anything to do with the product/service side,” Harkins says. “Even if it’s not a direct reporting relationship, there needs to be a relationship between the two sides, so we are looking at things holistically.”

2. View security as risk management

When a security breach does happen, it can put companies in the embarrassing position of having to explain why they weren’t better prepared. Repairing the damage often ends up costing a lot more than taking proper precautions would have in the first place.

Viewed this way, security is just another type of insurance. “What you are insuring against is protecting your reputation from a data breach,” says James Stansberry, SVP and head of Samsung ARTIK Smart IoT Platform, a division of the Korean electronics giant that makes IoT security and cloud solutions. “People just have to decide how much insurance they want.”

One way to weigh that decision is to look at what role a device plays in the IoT ecosystem. “There is no security that is new for IoT,” one security executive at a medical device manufacturer told us. To this executive, it’s a matter of asking the right questions: “What is the data you are collecting? Where are you sending it? Can someone use it for unintended purposes? In healthcare, we look at those things every time we create a medical product.”

This executive brings up the example of a device that is monitoring someone’s vital signs and dispensing drugs based on that information. Because a human life is on the other end, it is essential to encrypt the data being sent. But if the wireless range of the monitoring device is only five feet, then there is no need to worry about someone taking over the device for a DDoS attack.

But medical equipment is a different matter than most IoT devices. The chief security officer at a major vendor of enterprise software says that while consumer device makers have little incentive to improve security (because it’s not a “feature” most consumers demand), enterprises are much more concerned.

“There are some seismic shifts in the threat landscape in the past seven years,” this executive says, noting that financially motivated hackers have gotten much more sophisticated. “We were dealing with a bunch of JV players, and we’re now playing varsity.”

And these newly sophisticated attackers are focusing on the weak spots, such as companies' IoT infrastructure, which includes a lot of what has traditionally been considered "physical security"—wireless access cards, audio conference systems, HVAC systems, and the like.

Martin Bally, CSO at Diebold Nixdorf, a company that makes and services ATMs and point-of-sale systems, believes eventually customers will demand security in their products. "With IoT, there is a potential for a cyber attack to affect human safety," he says. "Once consumers start demanding that security, and regulations come into play, we'll see companies integrate security into their products more routinely."

3. Follow best practices

While connected devices expand the attack surface, many of the threats, like DDoS attacks, are the same ones the industry has been dealing with for decades. That's why adhering to best practices (changing default settings on devices, securing data in the cloud, encrypting data in transit, and so on) is so crucial.

The issue of securing connected devices has become such a concern that the government has stepped in and recently released "Strategic Principles for Securing the Internet of Things" (DHS, 2016). The document underscores the dangers of IoT and emphasizes how important best practices are in keeping data secure.

The problem is, because many connected products are inexpensive to build and follow a tight time-to-market, best practices like these often get brushed aside. To keep profit margins high, some companies simply accept they may get hacked.

"Some companies have given up on preventing problems and figure their only hope is to minimize damage by detecting sooner," says Cylance's Harkins. "If the measurement for a company is to limit liability, you are going to expose your customers more than necessary." Harkins feels companies are morally obligated to do the best job possible.

Meeting the talent challenge.

CSOs need to be mindful that recruiting top IoT security talent won't be easy. Cyber security talent is in short supply, and today's modern security challenges require a different perspective.

Skill sets are different than in other industries

Digital security professionals need to possess a wide range of skills. Beyond the usual technical know-how, they also need good business acumen and strong communications skills. That combination is not always easy to find.

IT departments historically operated in silos. Now they have to solve business problems, and that requires a different type of problem solving.

"Security folks tend to want to solve the problem like security folks, when we actually have to think like business people," explains the security officer at the medical device manufacturer. "Just because there is a vulnerability doesn't mean the world is going to end or we have to recall a product. It's understanding what it takes to build things."

The executive looks for people who don't give up on finding an answer to a problem. "It is the person who goes through all the scenarios and is looking for that needle in a haystack. And not being that know-it-all security person, but to be able to listen, work, and collaborate," the executive says.

Cylance's Harkins also stresses the importance of understanding the business. "When it comes to embedding technology into toys, you have to understand the manufacturing and design cycle," he says. "If you haven't

spent time on the product-creation side, you are going to have to overcome that experience gap pretty quickly."

Develop alternative talent pools

One way to locate good talent is to look outside the usual sphere. Samsung ARTIK's Stansberry looks for people in the financial industry, because finance has been working on tough security issues for a long time. "Standards committees are another good source of recruits," he says. "They become useful when you are trying to secure an ecosystem."

At the medical device maker, the security executive took a different approach to learning from outside of the industry. When this executive's group was looking to build a product security department, they weren't sure what was needed. So the exec recruited two employees to study security in other industries. "I sent them out for a year to find out what everybody else was doing, and then in a DevOps model, we helped build and define our own program," this executive says.

The enterprise CSO hires good technologists and then trains them internally. "I can teach security, but I can't teach technology," this executive says. "When you hire, your expectations need to be, 'I'm not going to find skilled labor in the market. I need to develop it myself,' so you need your own training process internally. Hire someone two years out of school, train them for two years, and they are good to go."

Training and retention programs to ensure ROI

A lot of money, time, and effort goes into training someone for a security role. Rather than watch that person hop to a new job six months later, smart CSOs look for ways to make sure they get a return on investment.

Diebold Nixdorf Bally looks for people who are in it for the long haul. “The market is so hot that people can easily jump ship and take a 10, 15, 20 percent bump in pay, and that is what they are doing,” he said. “We look for loyalty, longevity, and a culture fit. We really want someone who is going to be a long-term, part of the organization.”

One strategy Bally uses to make sure potential hires are a good fit is to have them meet with many people as possible. But still, it is not easy to find the right person. For example, it once took him 18 months to find a global security manager.

He also looks for creative ways, such as job rotations, to expose employees to different experiences and a variety of skills, because good salary isn’t the only thing people care about. They have to be stimulated in their work.

Conclusion

As senior security leaders face an expanding threat surface, combined with a growing scope of responsibilities, their roles are shifting. Instead of simply being responsible for network and data security, many CSOs' portfolios are now expanding to include physical security, IoT security, and the security of the increasingly connected products that their company produces.

As a result, CSOs need to get involved in product security early in the product-development cycle. They'll need to draw on a new set of skills themselves. For instance, many will need to strike a balance between time-to-market and security, or between security and bottom-line product costs. They will need to get comfortable negotiating with product-line leaders and the CEOs over features and security tradeoffs. And they will need to recruit new kinds of talent in order to meet the growing challenges of our increasingly connected world.

References

AT&T. 2016. "IoT evolution: Security trails deployment." AT&T. <https://www.business.att.com/cybersecurity/archives/v2/iot/>

DHS. 2016. "Strategic Principles for Securing the Internet of Things (IoT)." U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Gartner. November 2015. "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015." Gartner Inc. <http://www.gartner.com/newsroom/id/3165317>

Gartner. April 2016. "Gartner Says Worldwide IoT Security Spending to Reach \$348 Million in 2016." Gartner Inc. <http://www.gartner.com/newsroom/id/3291817>

Greenberg, Andy. August 1, 2016. "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse." Wired. <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>

Greenough, John. October 12, 2016. "How the Internet of Things is Revolutionizing Manufacturing." Business Insider. <http://www.businessinsider.com/internet-of-things-in-manufacturing-2016-10>

Hilton, Scott. October 26, 2016. "Dyn Analysis Summary Of Friday October 21 Attack." Dyn. <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>

Kassner, Michael. April 9, 2015. "Data breaches may cost less than the security to prevent them." Tech Republic. <http://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/>

Neustar. 2016. "Arm Yourself with New Research on DDoS Threats." Neustar. https://hello.neustar.biz/2016_ddos_report_security_lp.html

Polityuk, Pavel. December 20, 2016. "Ukraine investigates suspected cyber attack on Kiev power grid." Reuters. <http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF>

Acknowledgements

- Martin Bally, Chief Security Officer, Diebold Nixdorf
- Malcolm Harkins, Chief Security and Trust Officer, Cylance
- James Stansberry, SVP and head of Samsung ARTIK Smart IoT platform, Samsung

Contributors



Jamey Cummings
Senior Client Partner,
Co-leader, Global Security Practice



Aileen Alexander
Senior Client Partner,
Co-leader, Global Security Practice



Kevin Anderson
Principal, Internet of Things
Global Technology Practice



Louisa Perry
Senior Client Partner,
Lead, EMEA Security Practice

About Korn Ferry

Korn Ferry is the preeminent global people and organizational advisory firm. We help leaders, organizations, and societies succeed by releasing the full power and potential of people. Our nearly 7,000 colleagues deliver services through our Executive Search, Hay Group, and Futurestep divisions. Visit kornferry.com for more information.

About The Korn Ferry Institute

The Korn Ferry Institute, our research and analytics arm, was established to share intelligence and expert points of view on talent and leadership. Through studies, books, and a quarterly magazine, *Briefings*, we aim to increase understanding of how strategic talent decisions contribute to competitive advantage, growth, and success. Visit kornferryinstitute.com for more information.