Turnaround and transformation in cybersecurity: Financial services

Key findings from The Global State of Information Security® Survey 2016

As cyberattacks continue to escalate, forward-leaning financial services firms are beginning to leverage and link innovative cybersecurity tools, many of them cloud-enabled. These organizations are improving their security programs with technologies such as cloud-based cybersecurity services, Big Data analytics, and advanced authentication and biometrics.

Another measure of progress is a willingness to invest in cybersecurity. This year, average information security spending is up 14%.

The most significant cybersecurity challenges

1. Security protocols/standards of third-party vendors
2. Rapidly evolving, sophisticated, & complex technologies
3. Cross-border data exchanges
4. Increased use of mobile technologies by customers
5. Heightened information security threats from outside the country

The top challenge: Third-party security

Financial services respondents ranked assessment of security capabilities of third-party vendors as the top challenge to their information security efforts. Accordingly, more than half said they would increase spending to better monitor third-party security in the coming 12 months.

Others are improving third-party cooperation through the use of risk-based security frameworks. These guidelines can also help companies more easily exchange information with third-party business partners and suppliers, and communicate expectations and concerns about services that are being provided.

Use of mobile devices and payments mounts

Around the world, the use of mobile devices and apps for consumer banking has exploded. According to a study by Bain & Company, mobile is the most-used banking channel in 13 of 22 countries and accounts for around 30% of all interactions worldwide.[1]

To secure those interactions, financial services respondents say mobile device security is a leading spending priority in 2015. That's good news, given that exploitation of mobile devices has increased significantly in the past year. One way that financial institutions are tackling the rise in mobile risks is through the use of advanced authentication. Many banks, for instance, allow customers to access their accounts using biometrics like voice and facial recognition—an approach that is more convenient for consumers and improves security for financial firms.

In addition to mobile banking, consumers are embracing the use of mobile payment systems. Already, most financial services firms say they now accept some form of mobile payment. The next step will be to ensure robust, end-to-end security for these payment systems.

Complex attacks from abroad

Another top challenge for financial services firms is escalating security threats that originate in other nations. Much of the concern revolves around foreign nation-states, organized crime, and activist/hacktivist groups. The worry is certainly warranted: We have seen striking year-over-year increases in incidents attributed to these highly skilled adversaries.

Financial services companies have long dealt with sophisticated actors like organized crime, but some cite a worrisome trend: Certain threat actors seem to be working together to carry out attacks. For instance, company employees may be colluding with external adversaries like hacktivists. Perhaps even more menacing, some financial services executives believe that organized crime and foreign-nation states are joining forces to perpetrate cybercrime.

Many organizations are fighting back with the use of Big Data analytics to monitor for covert threats. Doing so has helped them better understand evolving external and internal security risks, as well as better monitor user behavior and network activity.

pwc

1 Used with permission from Bain & Company, *Customer loyalty in retail banking: Global edition 2014*, December 2014

How financial services organizations are responding to rising cyber-risks

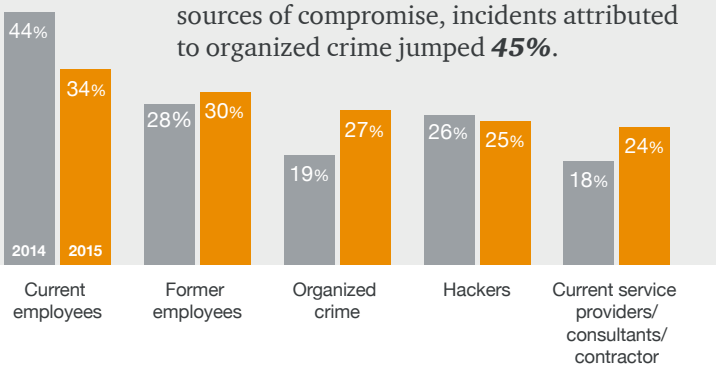
183%

Employee, customer, and "soft" IP data are the top three targets of cyberattacks, but theft of "hard" intellectual property soared **183%** in 2015.

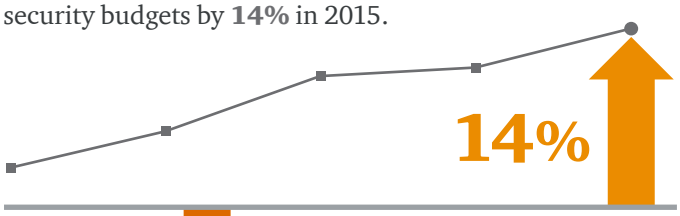
3%

In 2015, respondents detected **3%** fewer information security incidents than the year before.

While employees remain the most cited sources of compromise, incidents attributed to organized crime jumped ***45%***.



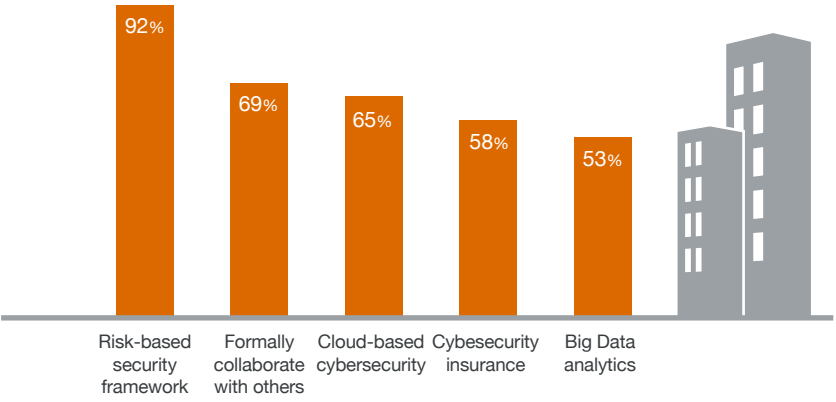
Accelerating last year's slight increase in security spending, respondents boosted their information security budgets by **14%** in 2015.



-12%

Estimated financial losses as a result of all security incidents declined **12%** over the year before.

Many organizations are implementing strategic initiatives—such as risk-based frameworks and cloud-enabled cybersecurity—to improve security and reduce risks.



Businesses are investing in core safeguards to better defend their ecosystems against evolving threats.

For a deeper dive into the 2016 Global State Information Security Survey findings go to pwc.com/gsiss or contact:

Joe Nocera
Principal, Cybersecurity and Privacy
+1 (312) 298 2745
joseph.nocera@pwc.com

Source: The Global State of Information Security® Survey 2016