Turnaround and transformation in cybersecurity: Power and utilities

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

Power and utilities organizations are facing a raft of challenges as a result of evolving business models, distributed generation and increasing demands of customers who want to use account information to manage their energy consumption.

As utility assets and systems are increasingly interconnected and generate more data, these systems and information assets are more at risk. In fact, compromise of customer records soared 62% in 2015—despite a significant drop in the overall number of security incidents detected, according to The Global State of Information Security® Survey.

At the same time, power and utilities organizations should safeguard their operational systems from highly skilled nation-state actors that may attack power grids as an act of cyberwarfare. It's a risk that is quickly rising: Survey respondents told us that compromise of operational systems more than doubled in 2015 and that exploits of embedded systems quadrupled.

Safeguarding cyberassets and data from cyberattacks is an important part of customer trust, business integrity and even national security. To do so, power and utilities companies are proactively implementing technologies such as cloud-based cybersecurity, Big Data analytics and advanced authentication. Additionally, more organizations share cybersecurity threat intelligence than ever before.

Another sign of progress is a continued willingness to invest in security: Organizations raised their information security budgets by 9% in 2015, the third consecutive year of information security spending increases.

Protecting the assets that matter

For years, current employees have been the most-cited source of cybersecurity incidents. They still are, but this year we saw a startling increase in incidents attributed to technically proficient threat actors like foreign nation-states, organized crime and terrorists. Not surprisingly, this advancement in incidents corresponds with a dramatic rise in theft of intellectual property as well as exploits of operational and embedded technologies mentioned above.

Power and utilities organizations are addressing the changing cast of cyberthreat actors by adopting innovative technologies. This year, we saw a spike in the use of Big Data analytics to better safeguard customer data, intellectual property and operational systems. Among the 55% of respondents who leverage Big Data, most told us that analytics has helped increase awareness of external and internal security threats, as well as helped enhance understanding of user behavior and anomalous network activity. These capabilities can help monitor for data breaches in progress, whether perpetrated by highly skilled external adversaries who may be attempting to disrupt the power grid or by internal employees who inadvertently leak data.

Another way that companies keep an eye on suspicious user and network activity is through the use of cloud-enabled cybersecurity services. Of the two-thirds of organizations that have adopted cloud-based security, real-time monitoring and analytics is the most frequently leveraged tool. Respondents also told us that advanced authentication technologies like cryptographic keys and software tokens have helped improve customer confidence in the company's cybersecurity and privacy capabilities—a key objective for digital utilities.

The human side of cybersecurity

Technology alone will not eliminate all cyber-risks. That's why many companies are also addressing the human aspects of cybersecurity.

Increasingly, power and utilities organizations are sharing cybersecurity threat intelligence with external partners to better identify and respond to risks. In 2015, the number of companies that collaborate on cybersecurity practices soared 88% over the year before. More specifically, the number of organizations that participate in industry or government information-sharing organizations more than doubled.

Internal collaboration also is on the rise as more Boards of Directors become involved in security issues. Participation is highest in discussions on information security budgets, but we saw the biggest jumps in Board involvement in security technologies and testing. The most-cited benefit of Board involvement? Increased funding for information security programs.

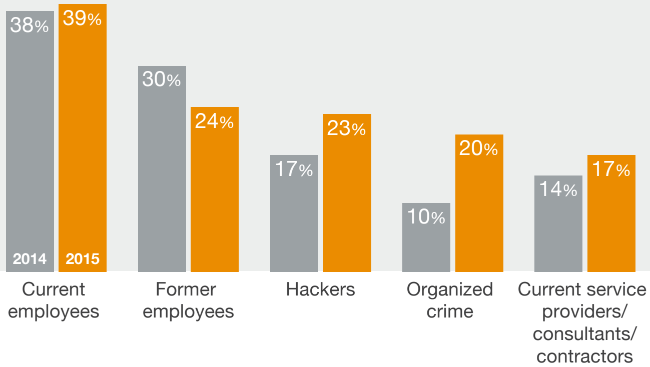
pwc

How power and utility organizations are responding to rising cyber-risks

234% While employee and customer records remain the top targets of cyberattacks and continue to increase, theft of "hard" intellectual property tripled in 2015.

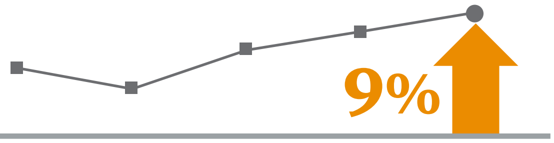
-36% Following a huge increase in 2014, the number of detected security incidents dropped **36%** in 2015.

Employees remain the most cited sources of incidents, but the number of respondents who attributed compromises to organized crime doubled in 2015.



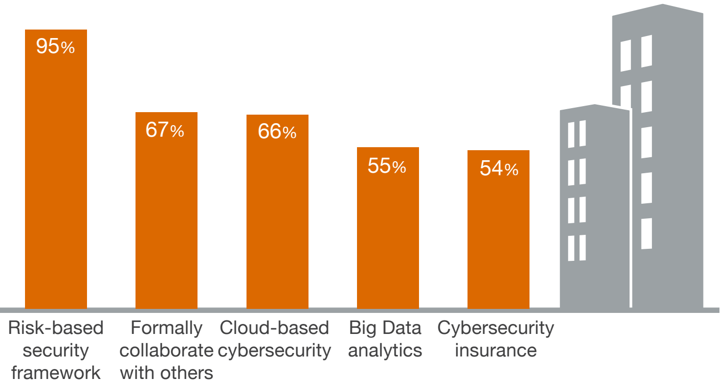
95%

Estimated total financial losses as a result of all security incidents almost doubled over the year before.

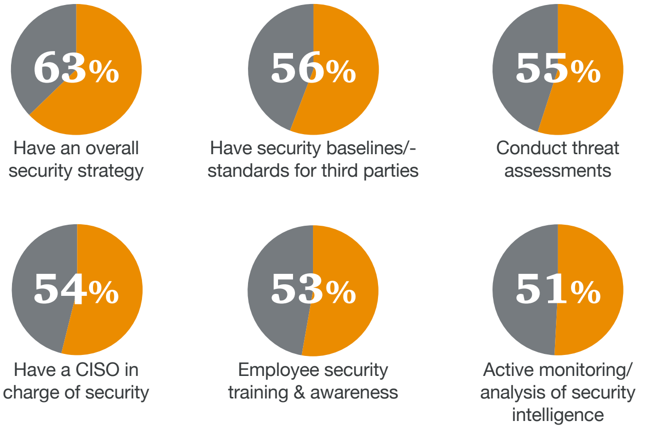


Continuing two years of increases in security spending, respondents raised their information security budgets by **9%** in 2015.

Many organizations are implementing strategic initiatives—such as risk-based frameworks and external collaboration—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:

Brad Bauch
Principal, Cybersecurity and Privacy
+1 (713) 356 4536
brad.bauch@pwc.com

Source: PwC, CSO, CIO, *The Global State of Information Security® Survey 2016*, October 2015