Turnaround and transformation in cybersecurity: Industrial products

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

Manufacturing stands on the threshold of profound change: The confluence of cloud computing, Big Data analytics, sensor-based technologies, 3D printing and robotics is beginning to transform the way products are developed, manufactured and sold. At the same time, manufacturers are broadening their business models by offering new technologies and services, as well as monetizing data generated by the products they produce.

This interconnected ecosystem of data-driven technologies—essentially, the Internet of Things (IoT)—will bring enormous efficiencies but it also will open new avenues of cybersecurity risks. Already, manufacturers report that security compromises of IoT technologies like operational systems and embedded devices more than doubled in 2015, according to The Global State of Information Security® Survey.

Forward-leaning organizations are taking steps to capitalize on the opportunities of IoT while leveraging innovative cybersecurity technologies and solutions, many of them cloud-enabled, to manage potential risks. These businesses are improving their security programs with technologies, including cloud-based cybersecurity services, advanced authentication and Big Data analytics. The vast majority of organizations also have adopted risk-based cybersecurity frameworks such as the NIST Cybersecurity Framework or ISO 27001 to help guide their overall security practices.

Amid these signs of progress, however, one stubbornly counterintuitive fact remains: Survey respondents trimmed information security budgets in 2015, following a significant increase in spending the year before.

A strategy for the Internet of Things

Manufacturers are already deploying interconnected equipment and sensor-based devices across locations to more efficiently run plant systems and enhance operations and logistics. Many are also preparing for the inevitable rise in cybersecurity risks that will accompany these technologies.

A majority of organizations are developing strategies to secure these interconnected devices, equipment and data. In fact, roughly two-thirds of survey respondents either have an IoT security strategy in place or are currently implementing a strategy.

Big Data will get bigger

In 2015, half of survey respondents said they use Big Data analytics to model for and identify cybersecurity threats. The benefits include better understanding of external and internal security threats, enhanced visibility into anomalous network behavior and an improved ability to identify and mitigate incidents.

We are also seeing a synthesis of Big Data and cloud-enabled cybersecurity services. As the volume of data mushrooms, industrial manufacturers are shifting more data to cloud providers—and many will be swayed to link analytics with sophisticated cloud-enabled cybersecurity services. This year, more than two-thirds of respondents said they use cloud-based services like real-time monitoring and analytics, identity and access management, and advanced authentication.

Printing the future in 3D

While most businesses have yet to adopt 3D printing for high-volume production, the technology is poised to disrupt manufacturing as we know it. Already, 42% of industrial products respondents said they use or plan to use 3D printing in the manufacturing process.

This transformation, however, may increase risk to trade secrets and intellectual property. That's because 3D printers often encode intellectual property as part of printing instructions and, like any digital document, these files can be hacked. As theft of intellectual property increases, most industrial products companies seem to be taking the threats seriously: 74% said they have evaluated the increased risk of incorporating trade secrets in 3D printing digital files.

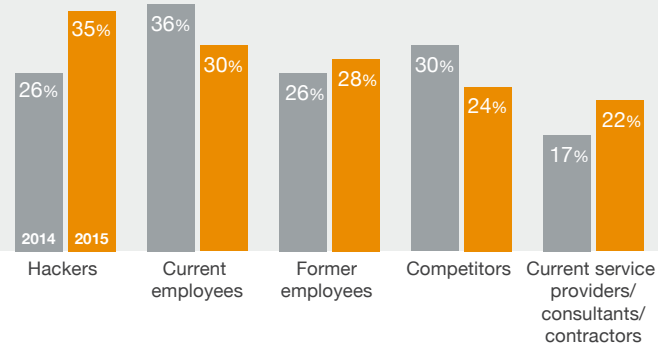
pwc

How industrial products manufacturers organizations are responding to rising cyber-risks

100% Theft of "hard" intellectual property (IP) such as product designs doubled in 2015, while loss of "soft" IP like business processes climbed **27%** over the year before.

-25% In 2015, respondents detected **25%** *fewer* information security incidents than the year before.

This year hackers are the most cited source of compromise, but the fastest growing sources of incidents are foreign nation-states.



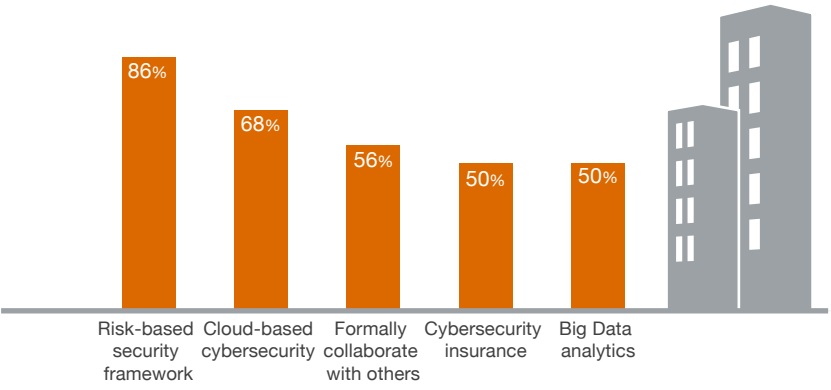
Estimated total financial losses as a result of all security incidents declined **24%** over the year before.

-24%

Following last year's significant increase in security spending, budgets dropped **15%** in 2015.

-15%

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:

Quentin Orr
Principal, Cybersecurity and Privacy
e.quentin.orr@pwc.com

Mark Ruiz
Director, Cybersecurity and Privacy
mark.a.ruiz@pwc.com

Source: The Global State of Information Security® Survey 2016

© 2015 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. 76502-2016 JP