Cybersecurity has become top of mind for most industrial products executives.

In the past year, the US Department of Justice charged five Chinese military hackers with conducting economic cyberespionage against six American organizations that included major manufacturers.¹ And the seemingly relentless assaults on major retailers, banks, and entertainment companies have heightened the awareness of cybersecurity risks across sectors and across the world.

Among industrial products respondents, the average number of detected security incidents climbed 17% over 2013, according to The Global State of Information Security® Survey (GSISS) 2015. This increase in security incidents comes at great cost: Our study of 557 industrial products executives found that total financial losses attributed to security compromises jumped 38% over the year before.

“Most industrial products companies don’t have sensitive consumer information to protect, but adversaries are interested in their intellectual property,” says Quentin Orr, an Advisory principal focused on cybersecurity and privacy. “We’re seeing IP sector clients wake up to this threat and take action.”

Current and former employees remain the most-cited sources of security incidents.

In 2014, we noted a considerable jump in incidents attributed to competitors, which more than doubled over 2013. Increasingly, industrial products executives believe that sophisticated international competitors are infiltrating their networks to pilfer trade secrets and manufacturing processes.

While incidents caused by employees often fly under the media radar, those committed by organized crime groups, activists, and nation-states typically do not. Attacks by these adversaries remain among the least frequent, but they are also among the fastest growing.

Cyber incidents attributed to nation-states, such as the Chinese hackers indicted by the US government, continue to garner the lion’s share of attention. Nation-states are keenly interested in manufacturing processes and they often attempt to steal intellectual property and trade secrets as a means to advance their own political and economic advantage. In 2014, compromises by foreign nation-states and foreign organizations increased 65% over 2013. Given the ability of nation-state adversaries to carry out attacks without detection, we believe the volume of incidents is very likely under-reported.

In 2014, 13% of respondents attributed security incidents to activists and hacktivists, a 61% jump over 2013. Similarly, the number of respondents who cited organized criminals as the source of attacks soared 54% over last year.
While incidents caused by employees often fly under the media radar, those committed by organized crime groups, activists, and nation-states typically do not. Attacks by these adversaries remain among the least frequent, but they are also among the fastest growing.

Cyber incidents attributed to nation-states, such as the Chinese hackers indicted by the US government, continue to garner the lion’s share of attention. Nation-states are keenly interested in manufacturing processes and they often attempt to steal intellectual property and trade secrets as a means to advance their own political and economic advantage. In 2014, compromises by foreign nation-states and foreign organizations increased 65% over 2013. Given the ability of nation-state adversaries to carry out attacks without detection, we believe the volume of incidents is very likely under-reported.

In 2014, 13% of respondents attributed security incidents to activists and hacktivists, a 61% jump over 2013. Similarly, the number of respondents who cited organized criminals as the source of attacks soared 54% over last year.

**GSISS 2015: Industrial products results at a glance**

« Click or tap each tile to view data

In 2013, 33% of respondents attributed incidents to former employees. In 2014, the percentage increased to 24%. In 2014, 26% of respondents attributed incidents to current employees, compared to 24% in 2013. The percentage of respondents who attributed incidents to competitors increased from 30% in 2013 to 28% in 2014. Similarly, the percentage of respondents who attributed incidents to hackers increased from 13% in 2013 to 26% in 2014.
While incidents caused by employees often fly under the media radar, those committed by organized crime groups, activists, and nation-states typically do not. Attacks by these adversaries remain among the least frequent, but they are also among the fastest growing.

Cyber incidents attributed to nation-states, such as the Chinese hackers indicted by the US government, continue to garner the lion’s share of attention. Nation-states are keenly interested in manufacturing processes and they often attempt to steal intellectual property and trade secrets as a means to advance their own political and economic advantage. In 2014, compromises by foreign nation-states and foreign organizations increased 65% over 2013. Given the ability of nation-state adversaries to carry out attacks without detection, we believe the volume of incidents is very likely under-reported.

In 2014, 13% of respondents attributed security incidents to activists and hacktivists, a 61% jump over 2013. Similarly, the number of respondents who cited organized criminals as the source of attacks soared 54% over last year.
Attacks spur security spending
As the frequency and costs of cyber incidents mount, companies are boosting their security budgets.

Among industrial products organizations, information security budgets increased 31% in 2014 over the year before, hitting an average of $5.2 million.

This boost follows an even larger 97% jump in security investments in 2013, which very well may account for a portion of the upsurge in detected incidents in 2014.

After all, our research shows that organizations that spend more on security typically discover more compromises.

Security budgets have increased by more than 150% over two years.

It’s also noteworthy that respondents’ security investments grew even as their overall IT budgets declined 25% over 2013. In fact, information security spending represents 6.9% of manufacturing respondents’ entire IT budget—up from 3.9% last year and the highest of any sector in our survey.

This indicates that, while industrial products companies have traditionally been a bit behind the curve in implementing up-to-date information security practices, they now understand the risks and are investing accordingly. The increases in security spending also suggest that those who deferred spending on security initiatives during the recession are now willing to spend as the economic recovery gains momentum.

Finally, the media spotlight on cybersecurity has intensified over the past year, and reports of high-profile retailer breaches, domestic surveillance snooping, and the government action against nation-state hackers have illuminated the potential for risks. As a result, many Boards of Directors are asking serious questions about information security preparedness.
Advances in key security initiatives

Increased security spending has resulted in some notable improvements in processes, technologies, and personnel training.

Nonetheless, there remains considerable room for improvement in security practices. Survey responses indicate that some critical initiatives have stalled or shown little advance over the past year. These include employee awareness and training programs, intrusion and vulnerability technologies, patch-management tools, and monitoring and analysis of security intelligence.

And even among the gains highlighted in the figure “Gains in security initiatives” on the following page, industrial products companies still lag in many areas. Consider, for instance, that businesses across industries are embracing external collaboration to improve security and threat intelligence, yet 45% of industrial products respondents have not begun to work with others. Also, the increasing risks of compromise by third-party vectors warrant a more firm commitment to due diligence of partners and supply chains.

It’s also worth pointing out that, while 61% of respondents now use some form of cloud computing, only 53% have a security strategy for the cloud.
Industrial products

Addressing security risks in an interconnected world // Key findings from The Global State of Information Security® Survey 2015

Advances in key security initiatives

* Have an overall information security strategy:
  - 2013: 77%
  - 2014: 81%

* Information security strategy is aligned to specific business needs:
  - 2013: 68%
  - 2014: 73%

* Employ Chief Information Security Officer (CISO) in charge of the security program:
  - 2013: 65%
  - 2014: 74%

* A senior executive communicates the importance of security across the enterprise:
  - 2013: 59%
  - 2014: 73%

* Business continuity/disaster recovery plans:
  - 2013: 54%
  - 2014: 72%

* Have an information security strategy aligned to specific business needs:
  - 2013: 50%
  - 2014: 58%

* Established security baselines/standards for external partners/customers/suppliers/vendors:
  - 2013: 58%
  - 2014: 64%

* Risk assessments on third-party vendors:
  - 2013: 45%
  - 2014: 55%

* Conduction of threat assessments:
  - 2013: 47%
  - 2014: 65%

* Have cyber insurance:
  - 2013: 50%
  - 2014: 66%

* Use mobile device management (MDM) solution:
  - 2013: 47%
  - 2014: 65%

* Program to identify sensitive assets:
  - 2013: 47%
  - 2014: 65%

* Conduction of penetration tests:
  - 2013: 48%
  - 2014: 59%

* Collaborate with others to improve security:
  - 2013: 45%
  - 2014: 55%

* Conduct threat assessments:
  - 2013: 47%
  - 2014: 65%

* Have cyber insurance:
  - 2013: 50%
  - 2014: 66%

* Use mobile device management (MDM) solution:
  - 2013: 47%
  - 2014: 65%

* Risk assessments on third-party vendors:
  - 2013: 45%
  - 2014: 55%

* Conduction of penetration tests:
  - 2013: 48%
  - 2014: 59%

* Collaborate with others to improve security:
  - 2013: 45%
  - 2014: 55%

* Program to identify sensitive assets:
  - 2013: 47%
  - 2014: 65%

* Establish security baselines/standards for external partners/customers/suppliers/vendors:
  - 2013: 58%
  - 2014: 64%

* Have an information security strategy aligned to specific business needs:
  - 2013: 50%
  - 2014: 58%

* A senior executive communicates the importance of security across the enterprise:
  - 2013: 59%
  - 2014: 73%

* Business continuity/disaster recovery plans:
  - 2013: 54%
  - 2014: 72%
Toward a more strategic approach

Organizations are revising their security programs to emphasize risk and top-down commitment.

Survey results indicate that many industrial product companies are beginning to rethink their approach to information security.

At the core of this initiative should be a risk-based cybersecurity program that enhances their ability to identify, manage, and respond to privacy and security threats.

A basic tenet of an effective information security strategy is that it should be anchored on the knowledge of what data is most important to the business. Because it is no longer possible to protect all information assets at the highest level, companies should precisely identify the information assets that are key to their profit and success—such as trade secrets, manufacturing processes, and product designs—and then prioritize protection of these assets.

“Every company has some trade secrets that allow it to make a profit, and the organization must identify and protect this information, because that’s what cyber adversaries will target,” says Orr of PwC. “You have to protect your future revenue streams.”

It’s an approach that companies are beginning to embrace.

In 2014, 61% of survey respondents say they have a program to identify sensitive assets, up from 49% last year. To help prioritize security protection, companies should classify the business value of data, a process that 69% of respondents currently have in place.

Next, organizations should strategically allocate security spending to the assets that are most valuable to the business. Industrial products respondents show an increasing commitment in this area: 66% say their security investments are allocated to the organization’s most profitable lines of business.

More organizations are protecting information assets based on their value to the business.
Cybersecurity and privacy should be embedded into an organization’s core, with a top-down commitment to security and ongoing employee training programs.

It was disappointing to find that the number of organizations that have employee security-awareness training programs (60%) remained static over last year. Considering that companies cite employees as the leading source of security incidents, we believe that training should be universal and that accountability should cascade from the C-suite to every employee and third-party vendor and supplier.

An effective security program also will require top-down commitment and communication.

Almost three-quarters (73%) of industrial products respondents have a senior executive—a Chief Operating Officer, Chief Financial Officer, or Chief Executive Officer, for example—who communicates the importance of information security to the entire enterprise, a healthy improvement over last year. This suggests that executive teams are starting to take ownership of cyber risks.

To do so, senior executives should proactively ensure that the Board of Directors understands how the organization will detect, defend against, and respond to cyber threats. Despite all the media attention following high-profile retailer and banking breaches, many companies have not yet elevated security to a Board-level discussion. Consider, for instance, that 53% of respondents say their Board of Directors participates in the overall security strategy and slightly fewer (48%) report the Board participates in the security budget. Only 33% say their Board is involved in reviews of current security and privacy risks—a crucial component of any effective security program.
Business partners under scrutiny

Due diligence is increasingly critical as organizations share more data with third parties.

As industrial manufacturing companies increasingly share data with a widening constellation of interconnected business partners, supply chains, and contractors, it is essential that they carefully assess the security capabilities of these third parties.

The logic is simple: As more data is shared through connected business ecosystems, more data is at risk of compromise.

In the past year, industrial products companies have stepped up due diligence of third-party and supply-chain partners. For instance, 64% say they have implemented security standards for external partners, suppliers, and vendors, up from 58% in 2013. And 58% of respondents say they perform risk assessments on third-party vendors, up from 50% last year.

These are solid improvements, to be sure, but it’s worrisome that approximately one-third of organizations have not addressed these issues.

Given that industrial products companies increasingly grow their businesses through mergers and acquisitions, comprehensive cyber due diligence of target firms is progressively important. Today, sophisticated cyber adversaries often infiltrate smaller, less-mature companies and lie in wait for them to be acquired by larger firms. When the companies’ information systems are integrated, threat actors may gain a foothold on the networks of the acquiring firms and attempt to exfiltrate trade secrets and other valuable information.

“When doing an acquisition, organizations should understand exactly what they are inheriting when they connect their networks with the company they acquire,” says PwC’s Orr. “This is a mature capability that very few manufacturing companies have developed.”

Evolving from security to cyber risk management

As security incidents continue to proliferate, industrial products companies are beginning to understand that cyber risks can never be completely eliminated. Protective measures remain important, of course, but processes and tools to detect, analyze, and respond to incidents are key to cyber resiliency and to the ongoing success of any industrial products manufacturing business.

To make this adjustment, industrial products companies should reposition their security strategy by integrating technologies, processes, and tools with the company’s broader risk-management activities. Doing so will result in a cyber-resilient program that can effectively manage threats based on the business’s tolerance for risk.
Contacts
To have a deeper conversation about cybersecurity, please contact:

Robert McCutcheon
Partner
412 355 2935
robert.w.mccutcheon@us.pwc.com

Quentin Orr
Principal
267 330 2699
c.quentin.orr@us.pwc.com

Bob Pethick
Principal
313 394 3016
bob.pethick@us.pwc.com

www.pwc.com/gsiss2015  //  www.pwc.com/cybersecurity

© 2015 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

PwC helps organisations and individuals create the value they’re looking for. We’re a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

PricewaterhouseCoopers has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PricewaterhouseCoopers gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.