THE CYBERSECURITY LITERACY CONFIDENCE GAP

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

Despite the fact that most organizations are more aware of cybersecurity risks than ever and are making significant investments in security technology, cybercriminals are targeting a broader set of corporate assets and using more sophisticated tactics to achieve their goals. Although organizations have improved their network defenses, many cyberattacks still remain undetected for more than eight months, and large-scale public breaches continue to dominate the news cycle. It's well understood that for every breach that is made public there are many more that go unreported either because they aren't detected or don't affect consumer data or critical infrastructure. As a result, organizations are not required to disclose them.

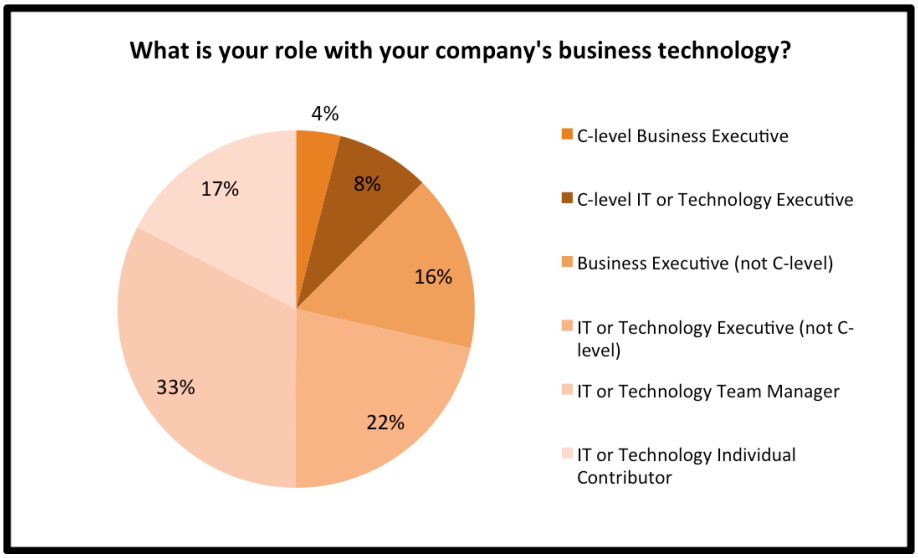
Leading companies tend to treat cyber risks in the same way they do other critical risks — primarily in terms of a risk/reward trade off. However, the sophistication of the attacks that corporations face today outstrips basic defenses, and as the complexity of these attacks increase, so does the risk they pose to corporations. In addition, competitive pressures to deploy cost-effective business technologies may affect resource investment calculations for security. These competing business pressures mean that conscientious and comprehensive oversight of cybersecurity risk at the board level is essential. However, it can be difficult for technical executives to accurately convey the changing shape of cybersecurity risks to non-technical executives.

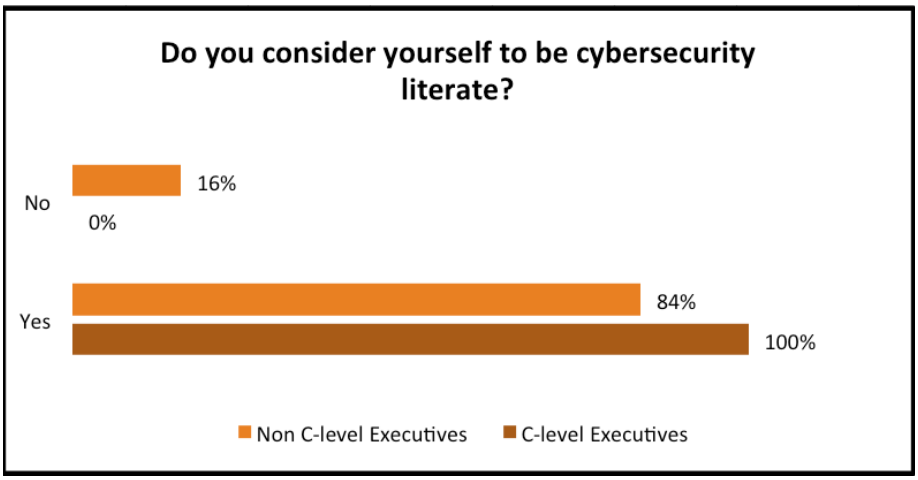
To understand how executives at leading companies view these risks, Tripwire sponsored a study of 200 business executives and 200 IT security professionals at U.S. companies with revenue over $5 billion per year. The study was conducted by Dimensional Research between February 15 and March 1, 2015.

The results of our study indicated that the levels of understanding of and confidence in cybersecurity literacy among boards and executives varied widely. Although all respondents considered themselves and their boards to be "cybersecurity literate," C-level executives were frequently the least confident in the cybersecurity information presented to their boards.

One-hundred percent of C-level executives and 84% of non C-level executives consider themselves "cybersecurity literate."

"There's a big difference between cybersecurity awareness and cybersecurity

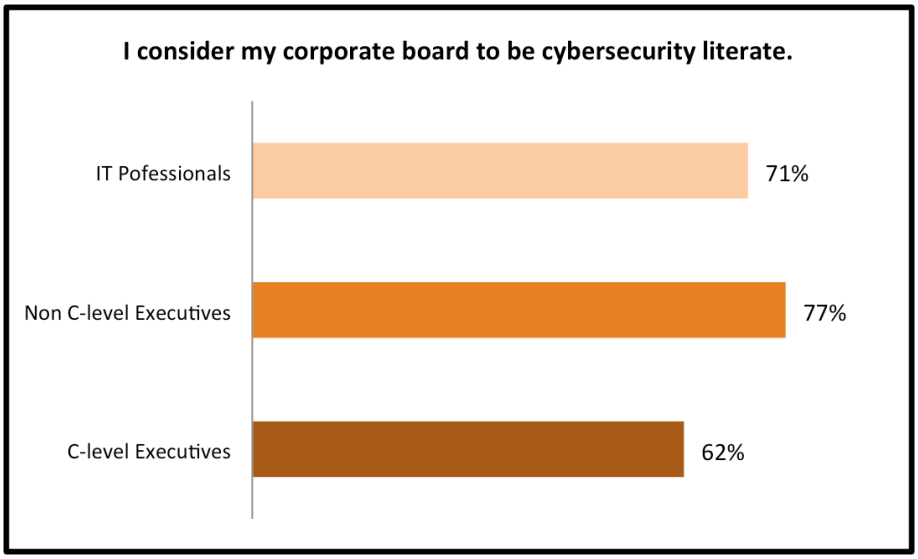


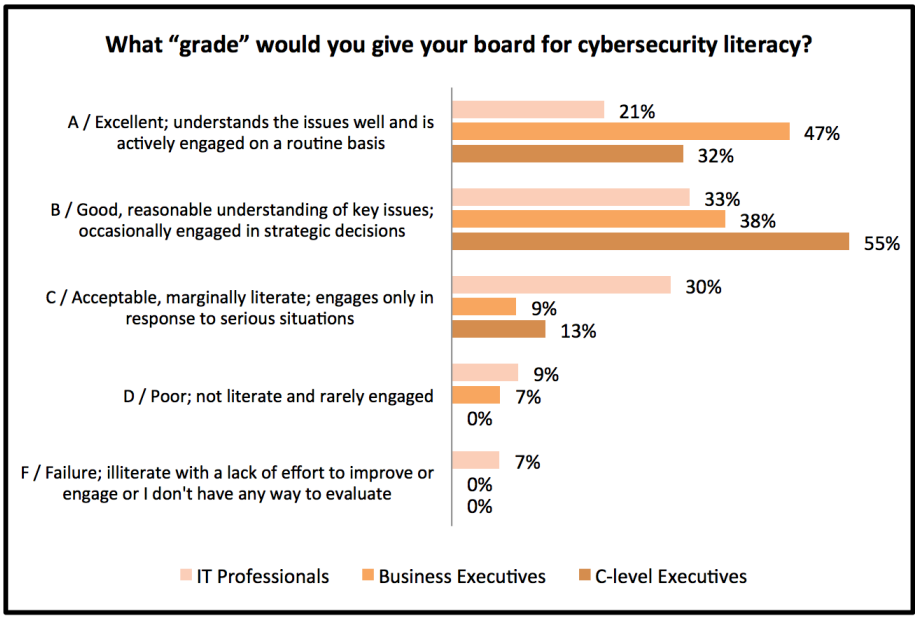


literacy," said Dwayne Melançon, chief technology officer for Tripwire. "If the vast majority of executives were really literate about cybersecurity risks, then spear phishing wouldn't work. I think these results are indicative of the growing awareness that the risks connected with cybersecurity are business critical, but it would appear the executives either don't understand how much they have to learn about cybersecurity, or they don't want to admit that they that they don't understand the business impact of these risks."

C-level executives are also significantly less likely than business executives to give their boards an "A" in cybersecurity literacy (32% and 47% respectively).

"It's surprising that so many executives give their boards a passing grade on cybersecurity," said Melançon. "This may reflect wishful thinking on the part of the executive staff. Boards are likely to evaluate cybersecurity risks from the perspective of defensible legal standards, and while this may be a useful exercise, it doesn't help determine acceptable levels of cybersecurity risk that can be used to guide day-to-day decision making."



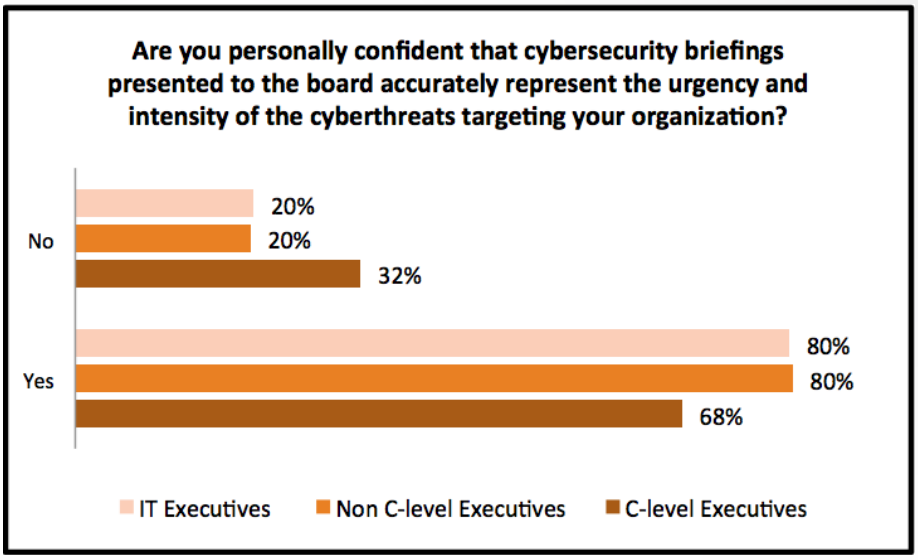


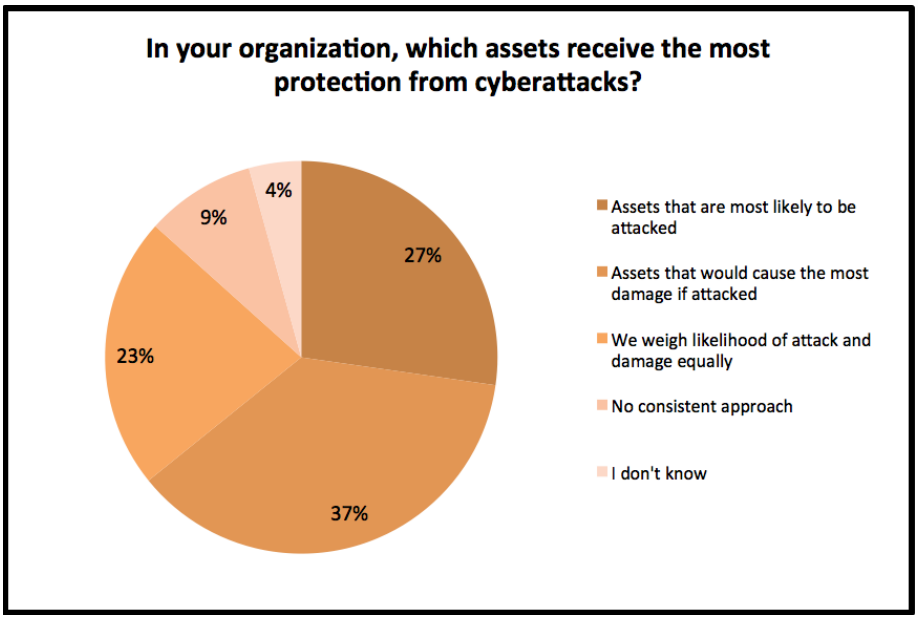
C-level executives were less confident than non C-level executives (65% and 87% respectively) regarding having the necessary tools to accurately present cybersecurity risks to the board. This is another area where they were noticeably less confident than IT executives (78%).

"Literacy and capability are not the same thing," said Tim Erlin, director of IT risk and security strategy for Tripwire. "In the case of cybersecurity risk, the industry lacks a clear set of standard metrics for measuring progress. The more technical the individual, the more likely they are to feel confident in the data, but many organizations find it difficult to translate the technical details into metrics that are meaningful to the business, let alone actionable at the executive and board level."

"It's clear that C-level executives consider cybersecurity risks as important as other business risks," said Chris Conacher, security research and development manager for Tripwire. "What's difficult is that they have few reference points for dealing with them. Whereas every executive will have a strategy for attacks by competitors or market forces, few have them for attacks by cybercriminals. On top of this, cybersecurity is such a nebulous problem that their own experts might not sound convincing when proposing risk management strategies. As a result, even the most able executives may be outside their comfort zone when it comes to decisions on cybersecurity risk."

C-level executives had less confidence than non C-level executives that cybersecurity briefings presented to the board accurately represented the urgency and intensity of the cyberthreats targeting their organizations (68% and 80% respectively).





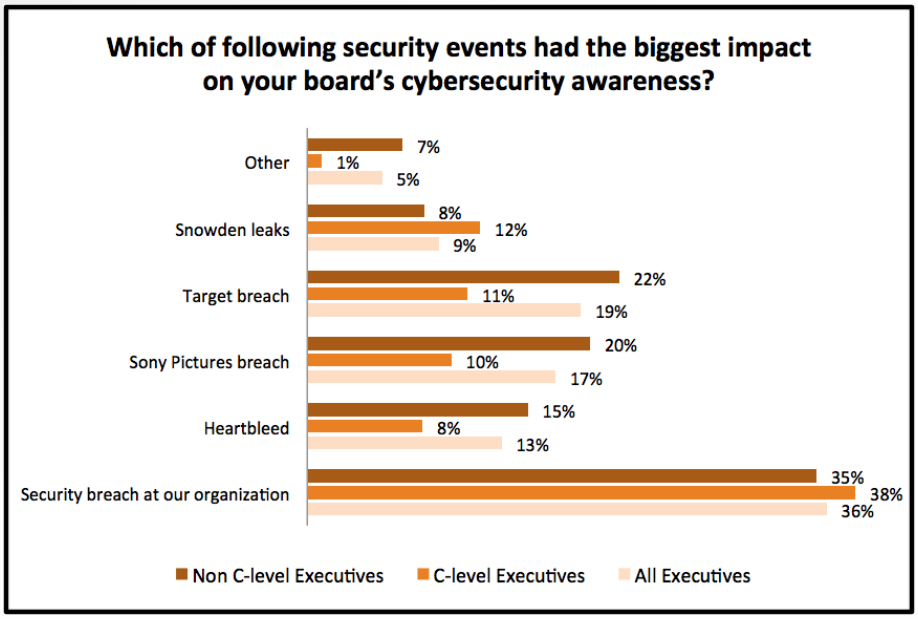
"The lower level of confidence on the part of C-level executives reflects a sea change in the way that cybersecurity risk is handled," said Melançon. "The reality is that an extremely secure business may not operate as well as an extremely innovative business. This means executives and boards have to collaborate on an acceptable risk threshold that may need to be adjusted as the business grows and changes. The good news is these results signal that a conversation is beginning to happen at all levels of the organization. This is a critical step in changing the culture of business to better manage the rapid changes in cybersecurity risks."

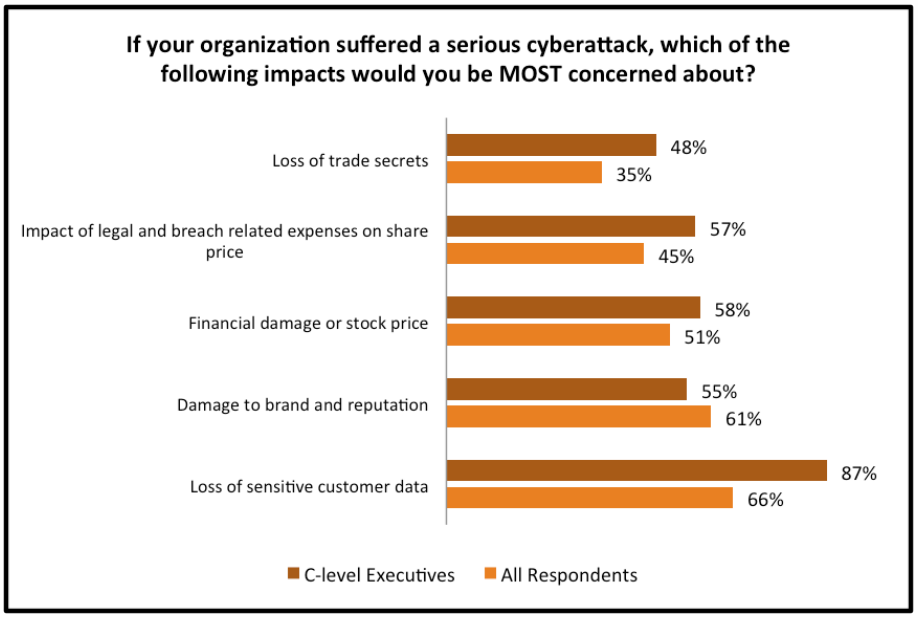
When asked about their strategy in protecting key assets, only 23% of all respondents said they would equally weigh the likelihood of attack with the impact of damage, and 9% said they had "no consistent approach."

"Identifying and protecting critical assets is a key component of any good information security strategy," said Erlin. "Not all risks are created equal, and an accurate assessment of an asset's value to the business can be challenging to obtain and maintain. Companies should think about the impact of damage as the flip side of business value in the risk equation."

All respondents agreed that a security breach at their organization had the biggest impact on their boards' cybersecurity awareness (36% for all executives). However, IT executives and IT professionals felt that Heartbleed had a much bigger impact (34%) than an internal breach (22%).

"The people closest to the work are most impacted by external security events that require a response," said Erlin. "IT professionals had to sit up, pay attention and apply patches for Heartbleed, even if they weren't under active attack. There weren't a lot of C-level executives who





spent the weekend running Heartbleed scans. An actual breach of your organization makes cybersecurity risk very personal in a way that can't be ignored."

C-level executives were most concerned about a loss of customer data during a breach and far less concerned about loss of trade secrets. Predictably, these executives were also concerned about brand and reputation damage, financial or stock price damage, and the impact of legal expenses and breach related costs on share price.

"When it comes to breach data, it's clear that customer data has the spotlight," said Erlin. "Executives are overwhelmingly aware of the risk that exposing customer data poses, in part because it's quantifiable, and in part because it's newsworthy. A breach with customer data invokes data breach notification laws and potential fines in some environments. It also makes headlines and drives lawsuits. While losing trade secrets is a risk, it's harder to model the outcomes."

According to Erlin, the difference in confidence between C-level executives and IT professionals is surprising. "In the majority of industry surveys we conduct, IT executives – who are dealing with risks in real-time and are fully aware of potential vulnerabilities, are less confident in their organizations' ability to withstand cybersecurity risks than their C-level counterparts. This survey found the opposite, and while the results point towards increased preparedness on the part of IT professionals, the low levels of C-level confidence points towards the need to increase board and C-level executive cybersecurity."

"I'm not surprised that C-level executives are less confident than their boards or IT executive staff. That lack of confidence comes, in large part, from the networking and informal benchmarking that takes place among C-level executives at the peer level. There is a lot of 'comparing notes' that happens between C-level peers. This could allow executives to get a more informed view of where they are in their overall cyber risk preparedness. This is in direct contrast to IT professionals who generally have a more insulated view of their own cyber risk, which can lead to a false sense of security. That difference in perspective—internal inputs vs. external inputs—may very well explain the confidence gap this survey highlights," concluded Melançon.

◆ Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

WPCLCG1c 201504