NEWS RELEASE

Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches And The Actions That Organizations Are Taking

2017-01-31

On 10th anniversary of report, classic attack vectors re-emerge; Cisco reduces "Time to Detection" to six hours

SAN JOSE, CA -- (Marketwired) -- 01/31/17 -- According to the Cisco® (NASDAQ: CSCO) 2017 Annual Cybersecurity Report (ACR), over one-third of organizations that experienced a breach in 2016 reported substantial customer, opportunity and revenue loss of more than 20 percent. Ninety percent of these organizations are improving threat defense technologies and processes after attacks by separating IT and security functions (38 percent), increasing security awareness training for employees (38 percent), and implementing risk mitigation techniques (37 percent). The report surveyed nearly 3,000 chief security officers (CSOs) and security operations leaders from 13 countries in the *Security Capabilities Benchmark Study*, part of the Cisco ACR.

Now in its 10^{th} year, the global report highlights challenges and opportunities for security teams to defend against the relentless evolution of cybercrime and shifting attack modes. CSOs cite budget constraints, poor compatibility of systems, and a lack of trained talent as the biggest barriers to advancing their security postures. Leaders also reveal that their security departments are increasingly complex environments with 65 percent of organizations using from six to more than 50 security products, increasing the potential for security effectiveness gaps.

To exploit these gaps, ACR data shows criminals leading a resurgence of "classic" attack vectors, such as adware and email spam, the latter at levels not seen since 2010. Spam accounts for nearly two-thirds (65 percent) of email with eight to 10 percent cited as malicious. Global spam volume is rising, often spread by large and thriving botnets.

Measuring effectiveness of security practices in the face of these attacks is critical. Cisco tracks progress in reducing "time to detection" (TTD), the window of time between a compromise and the detection of a threat. Faster time to detection is critical to constrain attackers' operational space and

minimize damage from intrusions. Cisco has successfully lowered the TTD from a median of 14 hours in early 2016 to as low as six hours in the last half of the year. This figure is based on opt-in telemetry gathered from Cisco security products deployed worldwide.

The Business Cost of Cyber Threats: Lost Customers, Lost Revenue

The 2017 ACR revealed the potential financial impact of attacks on businesses, from enterprises to SMBs. More than 50 percent of organizations faced public scrutiny after a security breach. Operations and finance systems were the most affected, followed by brand reputation and customer retention. For organizations that experienced an attack, the effect was substantial:

- Twenty-two percent of breached organizations lost customers -- 40 percent of them lost more than 20 percent of their customer base.
- Twenty-nine percent lost revenue, with 38 percent of that group losing more than 20 percent of revenue.
- Twenty-three percent of breached organizations lost business opportunities, with 42 percent of them losing more than 20 percent.

Hacker Operations and New "Business" Models

In 2016, hacking became more "corporate." Dynamic changes in the technology landscape, led by digitization, are creating opportunities for cybercriminals. While attackers continue to leverage time-tested techniques, they also employ new approaches that mirror the "middle management" structure of their corporate targets.

- New attack methods model corporate hierarchies: Certain malvertising campaigns employed brokers (or "gates") that act as middle managers, masking malicious activity. Adversaries can then move with greater speed, maintain their operational space, and evade detection.
- Cloud opportunity and risk: Twenty-seven percent of employee-introduced, third-party cloud applications, intended to open up new business opportunities and increase efficiencies, were categorized as high risk and created significant security concerns.
- Old-fashioned adware -- software that downloads advertising without user permission -- continued to prove successful, infecting 75 percent of organizations investigated.
- A bright spot emerged with a drop in the use of large exploit kits such as Angler, Nuclear and Neutrino, whose owners were brought down in 2016, but smaller players rushed in to fill the gap.

Secure the Business, Maintain Vigilance

The 2017 ACR reports that just 56 percent of security alerts are investigated and less than half of legitimate alerts remediated. Defenders, while confident in their tools, battle complexity and manpower challenges, leaving gaps of time and space for attackers to utilize to their advantage. Cisco advises these steps to prevent, detect, and mitigate threats and minimize risk:

- *Make security a business priority:* Executive leadership must own and evangelize security and fund it as a priority.
- *Measure operational discipline*: Review security practices, patch, and control access points to network systems, applications, functions, and data.
- *Test security effectiveness*: Establish clear metrics. Use them to validate and improve security practices.
- *Adopt an integrated defense approach*: Make integration and automation high on the list of assessment criteria to increase visibility, streamline interoperability, and reduce the time to detect and stop attacks. Security teams then can focus on investigating and resolving true threats.

Cisco Annual Cybersecurity Report - 10 Years of Data and Insights

Cybersecurity has changed drastically since the inaugural Cisco Annual Security Report in 2007. While technology has helped attacks become more damaging and defenses become more sophisticated, the foundation of security remains as important as ever.

- In 2007, the ACR reported web and business applications were targets, often via social engineering, or user-introduced infractions. In 2017, hackers attack cloud-based applications, and spam has escalated.
- Ten years ago, malware attacks were on the rise, with organized crime profiting from them. In today's shadow economy, thieves now run cybercrime as a business, offering low barrier-to-entry options to potential customers. Today perpetrators can be anyone, anywhere; they don't require a security background and can easily purchase "off-the-shelf" exploit kits.
- The 2007 report tracked 4,773 Cisco IntelliShield Security Alerts, mapping closely to the level seen by the National Vulnerability Database. By the 2017 report, for the same time period, the vendor-disclosed vulnerability alert volume had increased by 33 percent to 6,380. We believe the increase is driven by greater security awareness, an increased attack surface and an active adversary.
- In 2007 Cisco advised defenders to own a holistic approach to security, integrating tools, processes and policies, and educating stakeholders to protect their environments. Businesses looked to vendors for a comprehensive answer, often in vain, who instead prescribed piecemeal point solutions. In 2017 CSOs are grappling with the complexity of their environments. Cisco is combatting this through an architectural approach to security, helping customers get more from existing security investments, increasing capability while decreasing complexity.

Supporting Quotes
"In 2017, cyber is business, and business is cyber -- that requires a different conversation, and very different outcomes. Relentless improvement is required and that should be measured via efficacy, cost, and well managed risk. The 2017 Annual Cybersecurity Report demonstrates, and I hope justifies, answers to our struggles on budget, personnel, innovation and architecture."
- John N. Stewart, Senior Vice President and Chief Security and Trust Officer, Cisco

"One of our key metrics highlighted in the 2017 Annual Cybersecurity Report is the 'time to detection' -- the time it takes to find and mitigate against malicious activity. We have brought that number down to as low as six hours. A new metric -- the 'time to evolve' -- looked at how quickly threat actors changed their attacks to mask their identity. With these and other measures gleaned from report findings, and working with organizations to automate and integrate their threat defense, we can better help them minimize financial and operational risk and grow their business."
- David Ulevitch, Vice President/General Manager, Security Business, Cisco

About the Report
The *Cisco Annual Cybersecurity Report,* now in it's tenth year, examines the latest threat intelligence gathered by Cisco security experts, providing industry insights that reveal customer security trends. The 2017 report also highlights key findings from the third annual *Cisco Security Capabilities Benchmark Study* (SCBS), which examines security professionals' perceptions of the state of security in their organizations. It shares geopolitical trends, global developments around data localization, and the importance of cybersecurity as a boardroom topic.

For a complete copy of the 2017 Cisco Annual Security Research report, and to read more about Cisco's recommendations as to how businesses can mitigate against risk, click here.

Supporting Resources
Cisco Video with David Ulevitch, John N. Stewart: Cisco 2017 Annual Cybersecurity Report
Cisco 2017 Annual Cybersecurity Report
Cisco Blog: Staying Ahead of the Evolving Threat - Announcing the Cisco 2017 Annual Cybersecurity Report
Cisco 2017 Annual Cybersecurity Report Infographic
Cisco 2017 Annual Cybersecurity Report Graphics
Follow Cisco on Twitter @CiscoSecurity

Like Cisco Security on Facebook

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

RSS Feed for Cisco: http://newsroom.cisco.com/rss-feeds

Embedded Video Available

Press Relations
Ella Nevill
617-951-6622
elnevill@cisco.com

Analyst Relations
Jenna Duston
408-424 7210
jeabeyta@cisco.com

Investor Relations
Marty Palka
408-526 6635
mpalka@cisco.com

Source: Cisco