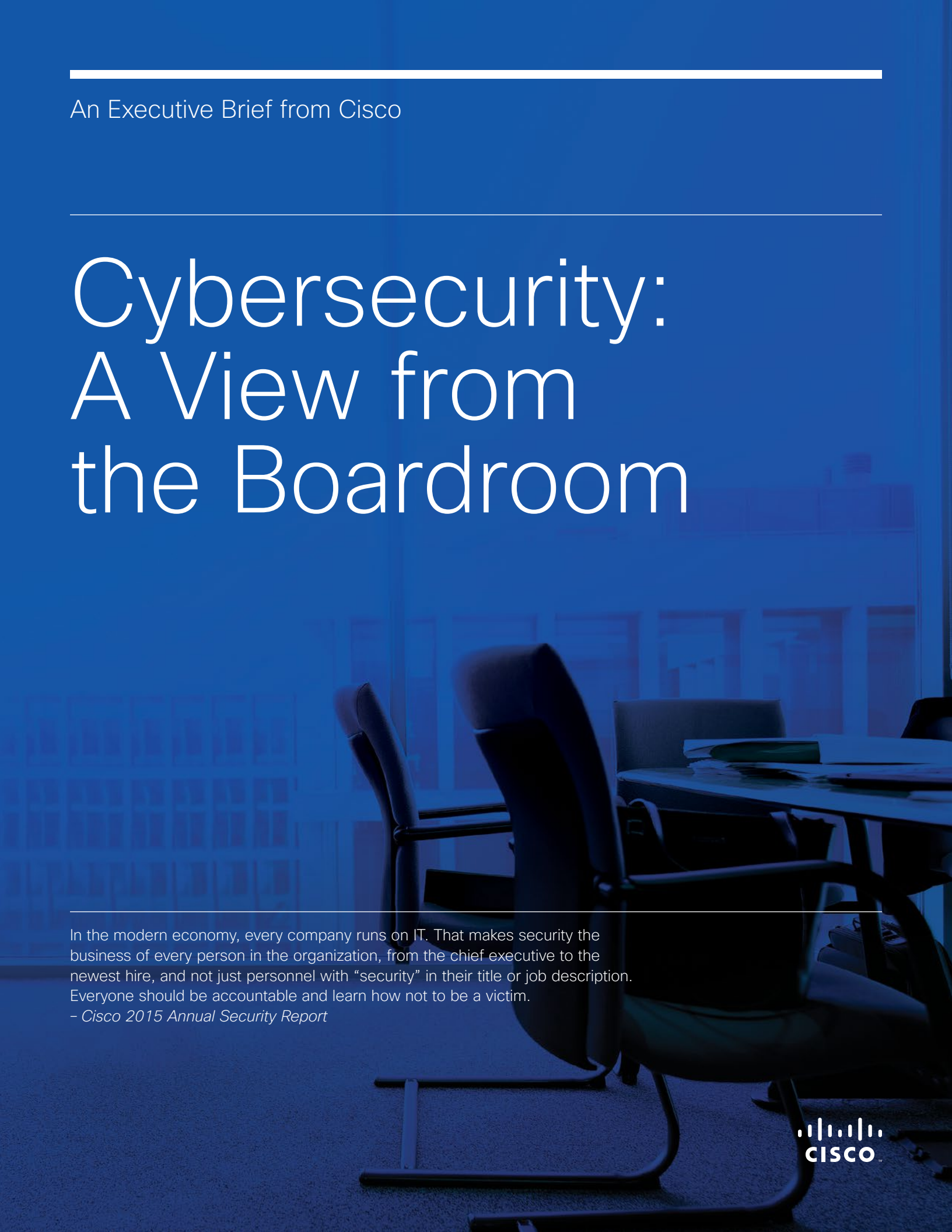
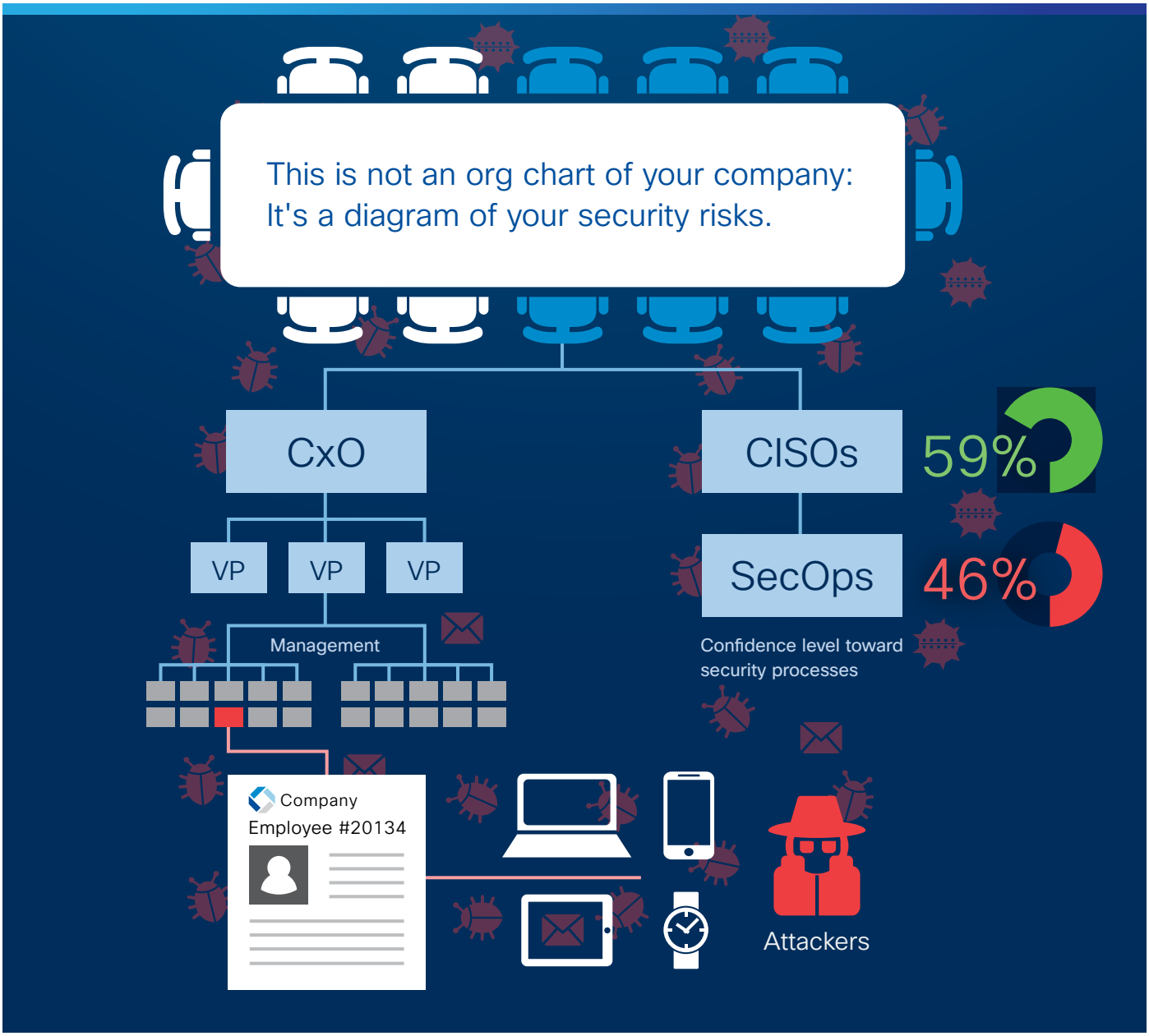
An Executive Brief from Cisco

Cybersecurity: A View from the Boardroom



In the modern economy, every company runs on IT. That makes security the business of every person in the organization, from the chief executive to the newest hire, and not just personnel with “security” in their title or job description. Everyone should be accountable and learn how not to be a victim.
– *Cisco 2015 Annual Security Report*

cisco



Security breaches are in the headlines and on your board members' minds. Cybercriminals are no longer fringe. They are an organized industry. High-profile breaches at well-known and respected government institutions and companies are becoming almost commonplace.

Commonplace and highly damaging. Beyond the theft of customer information, cybercriminals are creating legal issues, inciting fraud, and making off with intellectual property. And with the rise of social media, news of a breach can be difficult to contain. It carries inevitable damage to a company and its reputation.

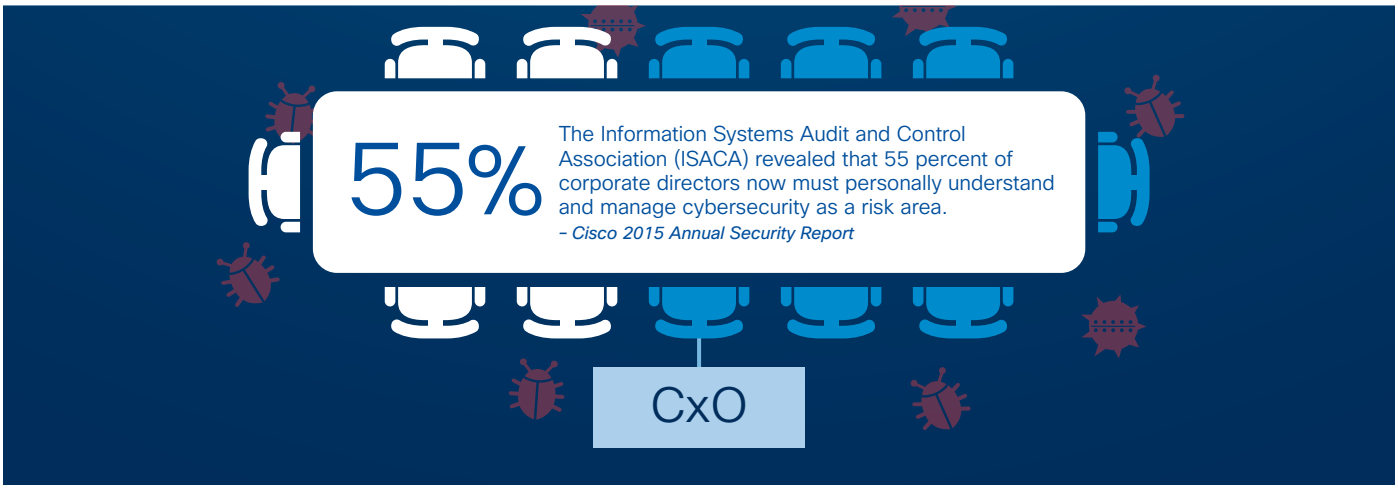
A Security Breach: Not If But When.

Although the tactics and methods of cybercriminals constantly morph, our *2015 Annual Security Report* provides insights that will help you prepare your organization, speak to the nature of the threats more intelligently, and understand how senior stakeholders in your own organization might comprehend and prioritize threats differently.

Included in this executive brief:

- **Page 2:** How to prepare yourself for greater boardroom engagement
- **Page 3:** How leadership within your organization—chief information security officers (CISOs) and security operations managers (SecOps)—might disagree on the threat level and what to do about it
- **Page 4:** How users have become unwitting accomplices of cybercriminals

Your board of directors: thinking about security like never before and coming with questions.



What's Going On?

Recent data breaches of well-known companies, data security regulation, and shareholder expectations are all bringing cybersecurity into the boardroom. Yet for many companies, this hasn't yet translated into action. How do you get out in front of your board's questions, invigorate the dialogue with correct information, and address its concerns?

Why Should It Matter to Me?

Ultimately every board has a fiduciary responsibility to its shareholders. Security concerns that once seemed peripheral have now come into stark focus. Cybercrime is affecting:

- **IP theft:** From patents to trade secrets to entertainment properties, IP is at risk.
- **Reputational damage:** Breaches not only scare customers but also are costly to repair.
- **Fraud:** Breaches frequently have the twin effect of diminishing trust and causing monetary loss.
- **Legal exposure:** Breaches create opportunities for lawsuits and their ensuing damages.
- **Financial losses:** Cybercrime's ripple effects damage a company's bottom line for years into the future.

What Should I Do Now?

1. Bring security into the boardroom as an ongoing agenda item and make an executive responsible for it.
Corporate boards of directors must know the cybersecurity risks to their business. To truly understand the scope of cybersecurity issues, boards should add members with technology and cybersecurity expertise.

2. Create a cyber-risk profile as part of the organization's overall risk assessment.
Cybersecurity is now directly tied to the health of an organization, affecting stock price. The board should determine avenues of cyber-risk, gather data, and evaluate probabilities. The resultant cyber-risk profile can inform the larger organizational risk assessment.

3. Get in front of questions from a newly engaged board by asking your security team the following questions:

- What controls do we have in place?
- How well have they been tested?
- Do we have a reporting process?
- How quickly can we detect and remediate the inevitable compromise?
- What else should we know?

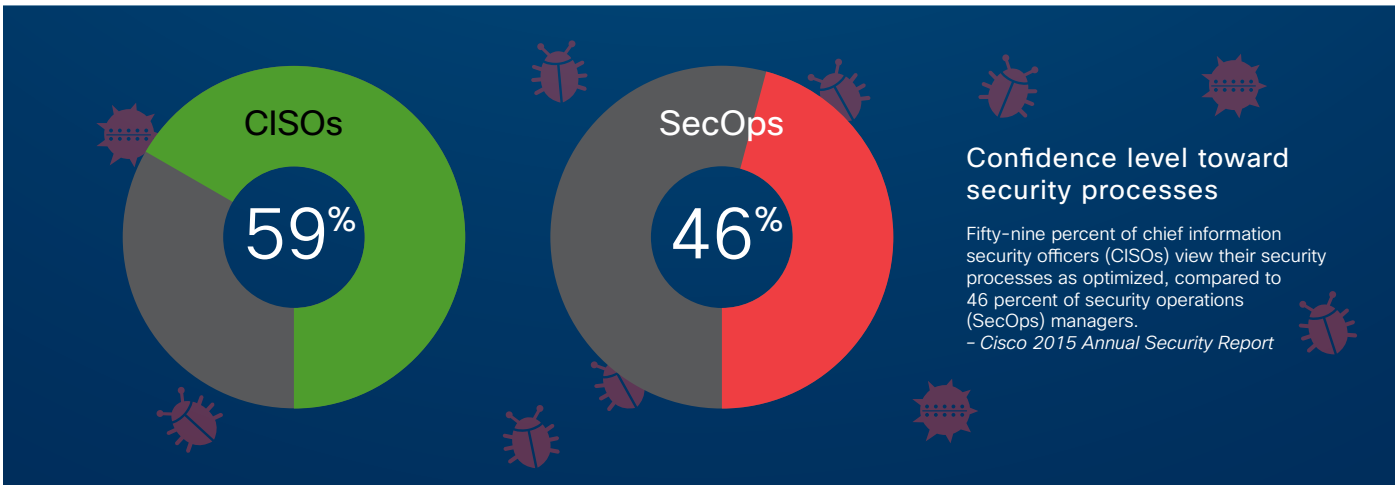
Be prepared to answer questions from the board in terms that are meaningful and that also outline business implications.

Is Your Industry a High-Risk Vertical?

To determine an industry's risk for malware encounters, Cisco Security Research examined eight types of attack methods. It found a perfect storm: the combination of targeted attack methods and careless user behavior online, with each having an impact on the level of risk.

Review Cisco's list of high-risk security verticals in *Cisco 2015 Annual Security Report.*

CISOs and SecOps: disconnected opinions



What's Going On?

Today's cybercriminals don't stand still. They constantly change tactics, probing the efficacy of each stratagem.

Amid this constant barrage, alignment across security leadership is crucial. However, CISOs are more optimistic than SecOps: 59 percent of CISOs strongly agree that their security processes are clear and well understood, but only 46 percent of SecOps agree.

Standard security tools are not always used. While 75 percent of CISOs see their security tools as being very or extremely effective, fewer than 50 percent of the respondents use the following basic methods:

- Identity administration or user provisioning
- Patching and configuration
- Penetration testing
- Endpoint forensics
- Vulnerability scanning

Why Should It Matter to Me?

Trusting your security doesn't change the numbers. Even if your organization blocks 99.999 percent of attacks, some will inevitably succeed. Focus on preparedness and put procedures in place to quickly respond when they do.

You might think your security is effective now, but it can soon be out of date. Attackers constantly change their strategies by:

- Disappearing from a network before they can be stopped
- Quickly choosing a different method to gain entry
- Using spam campaigns with hundreds of IP addresses
- Designing malware that relies on tools that users trust or view as benign
- Creating a hidden presence to blend in with your organization, sometimes taking weeks or months to establish multiple footholds

The disconnect between CISOs and SecOps in their opinions of threat levels and preparedness has consequences. For example, it can restrict resources to SecOps for what they believe is an urgent issue. If that issue becomes a confirmed crisis, it's more costly to contain, exposing your company, customers, and partners.

Vigilance must be relentless. Your team should understand that it's a constantly changing field of battle. The security practitioners you've hired should be held accountable to close the gaps.

What Should I Do Now?

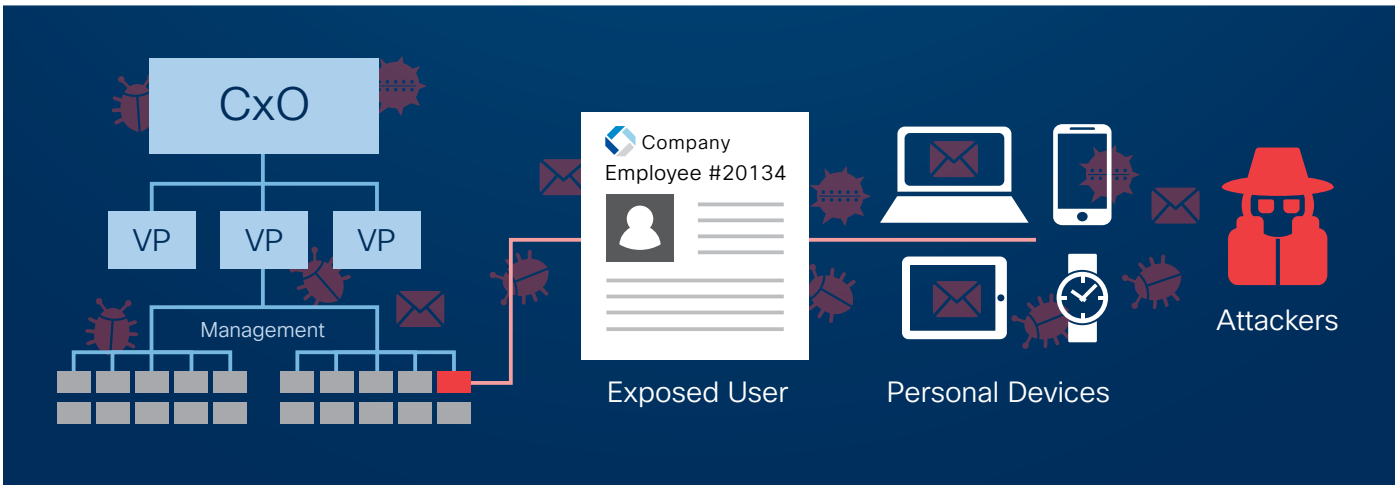
Align your team on the nature and strength of the threat landscape so resources are brought to bear where they're most needed.

Here are practical ways to evaluate the disparity of opinion within your organization:

1. Align business initiatives and security realities.
2. Implement policies that are in keeping with business objectives.
3. At a minimum, follow baseline security practices and raise your level of security maturity.
4. Realistically evaluate the effectiveness of the processes you're putting in place.
5. Revisit and optimize former and current processes.

Cisco 2015 Annual Security Report can inspire a candid discussion around our insights on threat intelligence and help close any disconnect within your security team.

Your users: unwitting enablers or empowered assets?



What's Going On?

Users are now unwitting enablers of attacks. While enterprises are busy blocking known threats, cybercriminals might send a fake request for a password – and a new breach begins. Security challenges affect several aspects of user behavior:

- **Failing to update browsers:** This error of omission enables more malicious attacks than would occur with automatic updates.
- **Clicking on spam:** Seemingly benign emails might contain a dangerous link or download of a malicious attachment.
- **Downloading from untrustworthy sites:** Users install PDF tools or video players downloaded from untrusted sources.
- **Trusting malvertising:** Users interact with seemingly legitimate advertising that leads them to download malicious software.
- **Using exploitable software:** Unpatched or outdated software provides adversaries with an easy path to attack users.

Why Should It Matter to Me?

The IoT is growing and creating a greater surface area to defend. Today there are 10 billion connected devices, a number that's expected to grow to 50 billion by 2020. The IoT enables business data to be passed back and forth in the cloud, creating a potential threat vector as users access company resources through personal devices.

Rogue applications are creating potential entry points for cybercrime. Malicious actors are using Web browser add-ons as a medium for distributing malware. This approach is proving successful because many users trust add-ons or view them as benign. In summary, increasing levels of access and resource demands on the network are the new reality – with ever-rising stakes.

What Should I Do Now?

With users increasingly becoming weak links in the security chain, you have choices to make:

- As software becomes easier to use, do you open new access-policy loopholes, only to have cybercriminals exploit them?
- Should you assume users cannot be trusted, and install stricter security controls?
- Or do you take the time to educate your staff and clearly explain how they play a vital role in achieving dynamic safeguards that support the business?

The Cisco Security Manifesto suggests the last option. Forcing users to work around new protocols that get in the way of their workday only leaves the business less protected. Creating your own security manifesto can help your users own the big picture.

The following are some pragmatic steps to implement with your security staff:

1. Understand the limitations of a porous network.
2. Segment the network and prioritize sensitive assets.
3. Train users on security policies and best practices.

