Mitigating the Cybersecurity Skills Shortage

Top Insights and Actions from Cisco Security Advisory Services

Cybersecurity Skills Are in High Demand, Yet in Short Supply

Increasingly sophisticated threat campaigns. High-profile data breaches. Determined threat actors. The sophistication of the technology and tactics used by criminals has outpaced the ability of IT and security professionals to address these threats.[1] *Security Magazine* reports that "most organizations do not have the people or systems to monitor their networks consistently and to determine how they are being infiltrated."[2] Cisco estimates there are more than 1 million unfilled security jobs worldwide.[3]

Determined attackers and persistent threats are only part of the cybersecurity skills problem. According to new research from Cisco, there is a disconnect between the perception and reality of security preparedness. While many chief information security officers (CISOs) believe their security processes are optimized–and their security tools are effective–their security readiness likely needs improvement.[4] This disconnect, along with rapidly evolving regulatory requirements and networking technology, will further widen the cybersecurity skills gap.

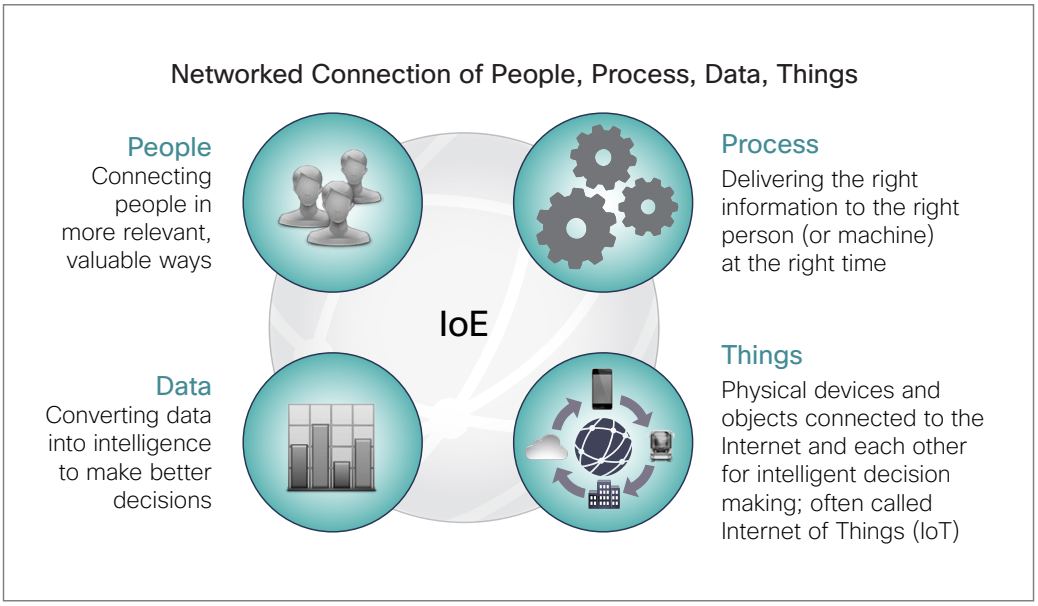
Cybersecurity hiring challenges will also be impacted by the Internet of Everything (IoE), which represents an unprecedented opportunity to connect people, processes, data, and things (Figure 1). While IoE will create new operating models that drive both efficiency and value, it may also become the world's most challenging cybersecurity threat.[5] Why? As customers embrace IoE, they must bring together IT and operational technology, giving adversaries new targets such as vehicles, buildings, and manufacturing plants.

> *Threats to critical OT (operational technology) infrastructure are no longer theoretical and their existing vulnerability is an area that actors are actively exploiting.*[6]
>
> – Michael Assante

This blurring of IT and operational technology environments has already resulted in a 250 percent spike in industrial automation and control system incidents over the past 4 years.[7] According to Gartner, the number, scale, and sophistication of operational technology attacks will continue to increase, putting connected industrial systems, building control systems, and energy systems at risk.[8] "Mitigating advanced persistent threats in OT environments requires people who can bridge IT and OT," says Jon Stanford, principal, Cisco® Security Solutions. People who can bridge the gap between IT and OT are in extremely short supply.

Against this dynamic backdrop, Cisco Security Services offer important insights and recommended actions that can help you mitigate the cybersecurity talent shortage.

Figure 1. With the IoT, Organizations Must Secure a Greater Attack Surface



> *"There is going to be a Black Friday–like buying frenzy for cybersecurity talent throughout 2015 … Some organizations will be left high and dry."*[9]
>
> – Jon Oltsik

As the Internet of Things (IoT) gains more traction, the lack of basic security standards in IoT devices will exacerbate the security skills gap.[10]

Insight Number 1

Cybersecurity Requires Cyber Strategies

Too many companies today have underperforming security programs because of a failure to define and execute holistic cybersecurity strategies. "A good cyber strategy should be a living, breathing, constantly questing process—not a task that is done every 6 months," says Brian Tillett, principal, Cisco Security Solutions. The lack of a cohesive, enterprisewide cybersecurity strategy, one that is based on policy, typically results in improvised security solutions that leave in-house security teams playing Whac-A-Mole. According to the *Cisco Security Capabilities Benchmark Study*, internal security teams spend 63 percent of their time on security-related tasks, leaving them little time to drive strategic security initiatives (Figure 2).[11]

Insight Number 2

Security Organizations Need Data Scientists with Business Acumen

With so many high-profile, high-cost breaches, business leaders are beginning to take notice. *Network World* says, "We're starting to see more executive-level emphasis on cybersecurity, more resources coming into cybersecurity, across all industry sectors. That has definitely increased the demand for cybersecurity folks."[13]

> *"Executive management and boards of directors are now recognizing that cybersecurity is not just a tech problem. It's a business problem."*
>
> — Ann Bednarz quoting Charlie Benway

As security discussions move to the boardroom, CISOs and their teams need data science skills to analyze cybersecurity data and business skills to manage trust (company reputation) and risk (costs). The new CISO must communicate not in bits and bytes, but in plain language. "The conversation has migrated from one of red, yellow, and green vulnerability status checks to financial conversations in which security risk is measured in dollars and cents," says Dmitry Kuchynski, principal, Cisco Security Solutions. "CISOs must be able to frame the discussion in a strategic way that clearly communicates the potential impact of a data breach on stock price, customer loyalty, customer acquisition, and the brand."

Figure 2. Security Resource Snapshot[12]

Insight Number 3

The Cyber-Talent Skills Gap Will Drive Enterprises to Managed Security Services

Most organizations are struggling to solidify a cybersecurity vision supported by an effective strategy that uses new technologies, simplifies their architecture and operations, and strengthens their security team.[14] This is pushing companies to bolster in-house cybersecurity expertise with professional security services (Figure 3).

More than 50 percent of organizations today seek advice or consulting services to help with their security strategies.[15]

Using security partners and managed security service providers (MSSPs) who continually invest in security expertise, intelligence, and innovative new technologies is a great way to keep pace with a dynamic threat environment. According to Jon Stanford of Cisco, "A trusted security advisor can help you establish a cybersecurity policy foundation and develop an effective cybersecurity program with the appropriate governance based on those policies." They can also take the burden of detection and triage off your hands, so your in-house security team can focus on remediation.

Insight Number 4

Effective Cybersecurity Requires People, Analytics, Intelligence, and Technology

Solving the growing cybersecurity problem requires more than skilled security professionals. It requires a combination of people, advanced analytics for proactive threat hunting, comprehensive intelligence for real-time threat awareness, and integrated security architectures.

This is why, according to Jon Oltsik of Network World, enterprises are shifting toward a new security model, one that is characterized by "central command-and-control and distributed enforcement, anchored by security intelligence and analytics." Oltsik writes that this relatively new technology model is "more art than science," and "CISOs need help in all areas of their planning here: design, test, implementation, integration, support, etc."

"Large organizations don't want to buy more one-off threat management point tools from a potpourri of vendors."

– Jon Oltsik

Insight Number 5

Every Company Is a Security Company

Security concerns are now top-of-mind not only for companies, but also for consumers. Cisco calls it "the trust problem." Simply put, breaches undermine confidence in both public and private organizations. This trust erosion leads to a decline in customer confidence in the integrity of your products. Without trust, customers will go elsewhere. As a result, all businesses need to think about security as their mainstream business.

Maintaining trust through state-of-the-art security capabilities can help you stand out in a crowded market. Innovative security-enabled solutions—such as mobile payments, virtual and automated advice, and customer collaboration tools—can create more valuable and relevant interactions. Differentiated security helps reassure customers and increase loyalty, and it can help you win in the IoE economy.

Figure 3. Findings from *Cisco Security Capabilities Benchmark Study*

Recommended Actions for Security Professionals

Action Number 1

Get a Cybersecurity Strategy

Dmitry Kuchynski of Cisco recommends that you "treat cybersecurity as if it were one of your solutions or services. When it comes to investor and customer confidence, security is just as important to the business." Cybersecurity strategies should be holistic. They should be:

- **Developed in collaboration with critical business units** – If your strategy is created in a vacuum, it will not align with business needs. Brian Tillett of Cisco recommends that you "embed security personnel into business units, so security strategy can be baked in instead of bolted on."
- **Focused on business growth** – If you bring value with your strategy, security becomes a business differentiator and revenue generator, transforming security from a cost center to a growth center.
- **Validated at the board level** – Executive leadership that prioritizes security is one of the signs of security sophistication, according to the *Cisco Security Capabilities Benchmark Study*. Keeping company executives informed and involved in data breach preparedness and response plans is essential for maintaining a sophisticated security posture.
- **Dynamically managed** – Threat actors continuously adapt. Your cybersecurity strategy should, too. Treat it like it is a living, breathing, constantly questing process. If you let it languish, your threat posture also suffers.

In addition, Jon Stanford recommends thinking broadly when formulating your strategy: "Cybersecurity is not just about IT. Your strategy has to include OT." Stanford also recommends performing risk assessments on third-party vendors, because you are only as good as your weakest link.

Action Number 2

Get a Breach Plan and Advanced Cybersecurity Skills

Even firms with mature security organizations and advanced security protocols will experience breaches, according to the Ponemon Institute. Every organization needs an incident response plan—a plan that maps out in advance and regularly tests against the types of incidents most likely for the firm's threat model.[16]

The Ponemon Institute recommends that you clearly define accountability and responsibility for data breach response and that it not be dispersed throughout the company. Instead, Ponemon advises creating cross-functional teams that include the expertise necessary to rapidly respond to a data breach. An effective incident response plan requires the skills of a variety of functions such as IT security, legal, and public relations.

Managed services from a trusted security advisor can help you create an incident response plan: one that uses the latest skills, analytics, intelligence, and technology to ensure rapid and effective resolution. Just make sure your security advisor or MSSP has deep knowledge of global enterprises.

You should take advantage of cybersecurity courses from vendors and certification groups to bolster in-house skills. The Cisco Learning Network now offers a new Cisco Cybersecurity Specialist certification for people who want to take on a first-responder role when networks have been attacked. Global Information Assurance Certification (GIAC) has a new Network Forensic Analyst certification that gives security professionals the skills to extract and analyze artifacts and activity left behind from unauthorized activity or network-based attacks.

Action Number 3

Get Security on the Agenda in the Boardroom

When it comes to getting executives engaged, Brian Tillett says, "Don't ever let a good breach go to waste." Tillett recommends using high-profile breaches as an opportunity to have a conversation with the board. Describe how that breach can happen in your organization. Then show them how to address vulnerabilities.

When it comes to finding CISOs with the business acumen to effectively engage with high-level executives, Dmitry Kuchynski recommends looking beyond security professionals for in-house hires: "Top-level candidates today come from military or federal enforcement

background, corporate technology, and security strategy experience because they have an understanding of the threat environment and bring a strategic mindset to the table." Kuchynski also recommends considering corporate security professionals who are moving laterally from small to large organizations and IT professionals who have made the move from the infrastructure to the security domain. If you are not successful in your CISO talent search, Kuchynski recommends partnering with a trusted vendor.

Action Number 4

Keep Your Security Solutions Operating at Peak Performance

Less than 50 percent of respondents in the *Cisco Security Capabilities Benchmark Study* use standard automation tools for identity administration or user provisioning, patching and configuration, penetration testing, endpoint forensics, and vulnerability. Greater use of automation tools not only improves your security posture, it frees your security staff to focus on more strategic initiatives.

Brian Tillett recommends the following: "Turn on more of the security features already integrated into your solutions. Organizations typically turn on only 30 percent of the security features available to them. This is a tremendous underutilization of security resources that can make already-constrained security teams more productive and existing security solutions more effective."

And keep your software current. Unpatched or outdated software represents an attractive attack surface for adversaries. According to Cisco security research, "The proliferation of outdated versions of exploitable software will continue to lead to security issues of great magnitude."[17]

Action Number 5

Choose the Right Partners

If every company is now a security company, choosing the right partner is paramount. Obtaining the right cybersecurity partner can help you round out your expertise, so you can be:

- **More dynamic in your approach to security** by benefitting from global best practices and real-time threat intelligence
- **More proactive in your security posture** by using advanced analytics capabilities
- **More adaptive and innovative than your adversaries** by implementing a threat-centric security program that can address the full attack continuum before, during, and after an attack across all attack vectors

> *"In advanced security analytics, the value comes from the people. Software does not provide the answers; it provides the tools and delivers the data needed to discover answers."*
>
> – *"Big Data" Analytics in Network Security*, Frost & Sullivan, Feb. 13, 2015[18]

For More Information

These are just a few of the many ways organizations can mitigate the cybersecurity skills shortage:

- Find more information about Cisco Security Services.
- Read the *Cisco 2015 Annual Security Report*.
- Get an overview of Cisco Advisory Services.
- Learn how the Cisco Managed Threat Defense Service can help you navigate a changing threat landscape.
- Find out more about the new Cisco Cybersecurity Specialist certification.

---

1 *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.
2 "Why the Security Talent Gap is the Next Big Crisis," *Security Magazine*, May 2014.
3 *Cisco Security Capabilities Benchmark Study*, Cisco, Oct. 2014.
4 *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.
5 *Cisco 2014 Annual Security Report*, Cisco, Jan. 20, 2015.
6 "Cyber Threats Providing Their Power over Power Plan Operational Technology," PowerMag.com, Feb. 1, 2015.
7 "Cyber Threats Providing Their Power over Power Plan Operational Technology," PowerMag.com, Feb. 1, 2015.
8 "Operational Technology Security and the Challenges Ahead for 2015," Gartner Blog Network, Dec. 29, 2014.
9 "Cybersecurity Skills Shortage Panic in 2015?," *Network World*, Dec. 9, 2014.
10 "2015 Security Predictions: IoT to Join Cloud Breaches and Ransomware," ZDNet, Dec. 19, 2014.
11 *Cisco Security Capabilities Benchmark Study*, Cisco, Oct. 2014.
12 *Cisco Security Capabilities Benchmark Study*, Cisco, Oct. 2014.
13 "Shortage of Security Pros Worsens," *Network World*, March 9, 2015.
14 *Cisco 2014 Annual Security Report*, Cisco, Jan. 16, 2014.
15 *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.
16 *Ponemon Institute Report: Cyber Security Incident Response – Are we as prepared as we think?*, Ponemon Institute, Jan. 2014.
17 *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.
18 *"Big Data" Analytics in Network Security: Computational Automation of Security Professionals*, Frost & Sullivan, Feb. 13, 2015.