IT and business management roles in cybersecurity

Cybersecurity with the right stuff: When IT and business management work together.

In this paper, we'll address how business and IT managers can work together to build and implement a cybersecurity plan. In subsequent papers, we'll discuss issues such as creating security policies, helping to ensure open communication, and other topics that will help you protect your organization from cyberattacks.

Note that a more detailed "Quick-Start Planning Tool: Checkup for Your Cybersecurity Team Strategy" accompanies this paper. It can be downloaded for printing and distribution at your organization's management meetings.

Today's IT teams are working in an increasingly complex cybersecurity environment. They need more resources—including specialized and certified teams to help keep their organizations safe. And they must be smart about building a plan and deploying necessary resources.

But CEOs and other managers may not understand the entire cybersecurity picture, and therefore, they may deny requests for more personnel, training, and other resources. Likewise, IT management may be at a loss to explain the business necessity of building an appropriate security team for the organization. How can these two groups create and work from the same set of priorities?

IT and business management roles in cybersecurity

First, let's agree that it is essential for an organization to create a cybersecurity team that can address several important issues, including:

What have you got to lose? What are you protecting?

Identify and catalog the organization's systems and information assets, including inventory, equipment, and customers, as well as softer assets, like reputation, goodwill, and credit rating.

Evaluate and prioritize those assets, understanding how big of an issue it would be for the organization to lose control or access, or to have those assets damaged.

What are your threats and risks?

Discover weak points, find and patch outdated and unpatched systems and applications.

Stay informed about new risks that face your organization. Your security team should have a reliable source of risk intelligence.

What are your obligations? What are your rules?

Understand and document policies and standards. These may include adherence to regulatory compliance and addressing responsibilities toward various groups, such as customers, vendors, distributors, and others. Costs of compliance violations can be significant.

What controls protect you? How do you know they're working?

Build and deploy security controls that enforce policies and processes to safeguard assets.

Monitor these controls to make sure they keep up with changing threats and requirements.

What skills does your team have? How are you growing team capabilities?

Hire the right people. Make sure that your organization is sufficiently staffed, with an appropriate variety of skills, experience levels, and outside support.

Continually expand skills and expertise to keep up with evolving threats. That may involve certifying existing staff, hiring those who are already certified, or contracting with certified consulting firms.

Build user awareness of security policies and standards. If employees don't understand and follow policies, that failure could become vulnerability. Trained users can help your capabilities.

What are you doing to keep up to date?

Plan and communicate with each other. Have a regularly reviewed set of plans to address the attack continuum.

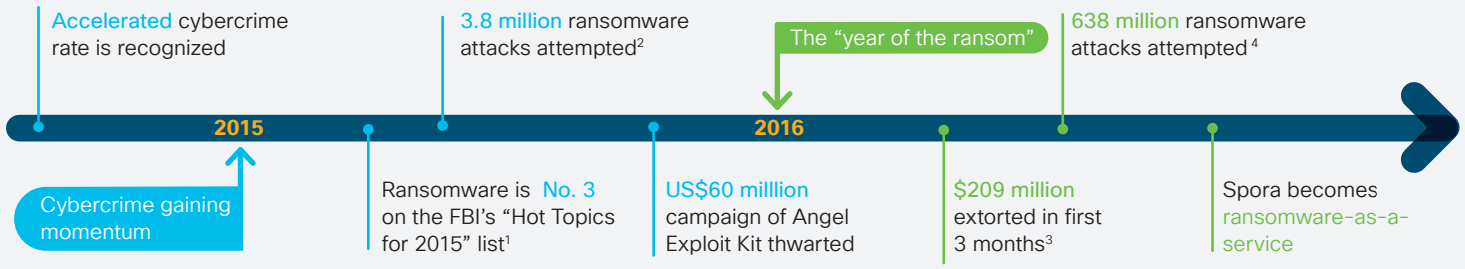
Review and reevaluate all steps on a predictable schedule, adjusting as necessary.

This may sound like a great deal of work—but rebuilding your organization after an attack will be far more labor-intensive and costly. Why? Because the threat landscape has changed dramatically.

Not very long ago, hacking was the primary concern. Typically, it was limited to a single individual testing his or her ingenuity at breaking into defended networks. It wasn't much different from an intruder unlocking the front door and wandering the halls. But this is no longer the case.

IT and business management roles in cybersecurity

Figure 1: Cybercrime is becoming big business



Cybercrime is now a lucrative global business

Here are some sobering facts. In recent years, cybercrime has moved from "mischievous teenage pranks" to become a multibillion-dollar business. It has very low margins, a low cost of entry, and a lucrative payoff. Cybercrime has become commercialized and profitable, with instructions publicly available on YouTube and other Internet sources.

In fact, any aspiring cybercriminal can purchase off-the-shelf ransomware and launch it inside a network—including your network. Often, all it takes is an unsuspecting employee clicking the wrong link in an email. Your operations will be shut down until you pay the ransom. The amount typically will be within your reach, but it will be sizable. Moreover, because cybercrime is rapidly expanding, it is attracting more criminals and increasing the chances that you'll be attacked.

US$24 million were extorted in 2015. But this amount increased to $209 million in just the first three months of 2016. Because of an expected increase to $1 billion in extortion profits, that year was designated as "the year of the ransom."

No longer are organizations safe if they simply build a better lock or a better wall around the proverbial castle. Now they need intrusion prevention and detection, not only at the perimeter, but also throughout the network. This means that, in addition to protecting that castle, they also must defend it when—not if—attacks are made.

It should go without saying that organizations should be aware of every intrusion, security incident, or other successful breach. But even the largest corporations have missed serious breaches, sometimes not becoming aware for weeks, months, or even years. These have caused significant loss of market value while endangering customer data, intellectual property, and more.

Cybercriminal teams often study the habits of specific organizations or types of companies so they can predict the best time to move—especially during weekends, holidays, and other times when fewer security people may be in place. If these people aren't trained to be just as alert during company down times, they'll become a point of vulnerability.

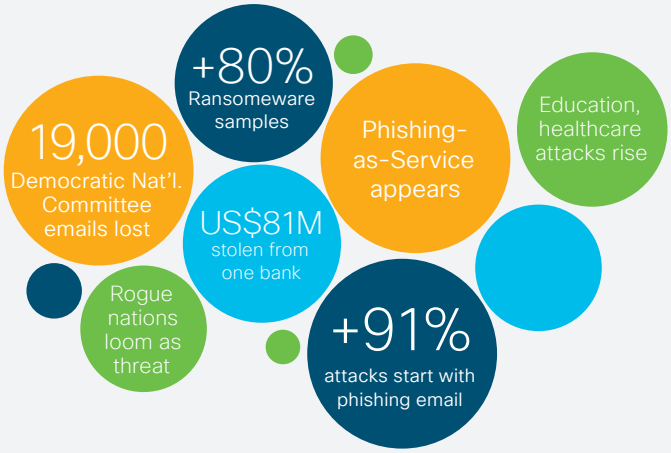
The threat landscape is rapidly evolving and expanding (Figure 2, see next page). One reason is because today's systems are becoming exponentially more complex. Just two decades ago, only three areas had primary security focus—client, server, and network. But now, the world's organizations are moving rapidly into digitization, they're using cloud-based storage, they're turning to on-demand services, and they're using virtualization. Automation alone offers special vulnerability because automated controls have the same permissions as an authorized administrator.

It is critical for management to consider all these parts and how they relate to security because many things can become weak points—including employees who could become unwitting targets of social engineering.

1. 2015 FBI Internet Crime Report.
2. Forbes, "2016 Saw an Insane Rise in the Number of Ransomware Attacks," February 7, 2017.
3. Ibid
4. Ibid

IT and business management roles in cybersecurity

Figure 2: Changing Threats in 2016[7]



Here's how the cybersecurity landscape is trending:

- Automated and scripted attacks move faster than ever before.
- Ransomware and extortion are on the rise.
- Malware is becoming more sophisticated (sandbox detection and more).
- Time-to-exploit announced vulnerabilities continue to drop.
- Hardly any organization is immune, and nearly every sector is a target: healthcare, retail, education, government, finance, and more.
- On a global basis, security and privacy regulations and laws have quickly become top growth areas.

Is it becoming obvious that today's effective cybersecurity protection involves much more than just technology upgrades, including firewalls and antivirus applications? In fact, an organization can no longer use the same ready-to-run protection it used years ago. A complete picture would include the right cybersecurity experts for the organization, a process for evaluating assets and threats, formalized policies and procedures, effective communications, and the type of teamwork that ties it all together.

It is like assembling a strong sports team in which everyone has a specific role and expertise. One or two people cannot compose the entire team. An organization needs trained and certified people who can be trusted to advise about all the moving parts, divide up the responsibilities, staff the appropriate levels, and implement a security budget.

Today's threats call for a sophisticated security approach

To begin with, today's requirements for hardening a system involve more than just a single security expert patrolling the organization's virtual hallways and jiggling doorknobs. Now it requires a complete team of experts who understand the many facets of cybersecurity. These may include experts who can:

- Understand and evaluate the growing number of security technologies and whether they fit the organization's requirements.
- Design and revise security architecture and the way it is controlled, and who understands that these requirements can change as attacks become more sophisticated.
- Deploy new systems according to best practices and the architect's guidelines.
- Understand secure access points, VPN operation, firewall technologies, content and endpoint security, cryptography, attack methods, host-based analysis, and other facets of cybersecurity.
- Set priorities and policies, plan and manage budgets, understand regulatory and legal compliance, appreciate business priorities and tradeoffs, and contribute at least several years of experience in security roles.

Finding those people may not always be easy. According to McAfee's Center for Strategic and International Studies (Hacking the Skills Shortage), the world will see a shortfall of two million cybersecurity experts by 2019.

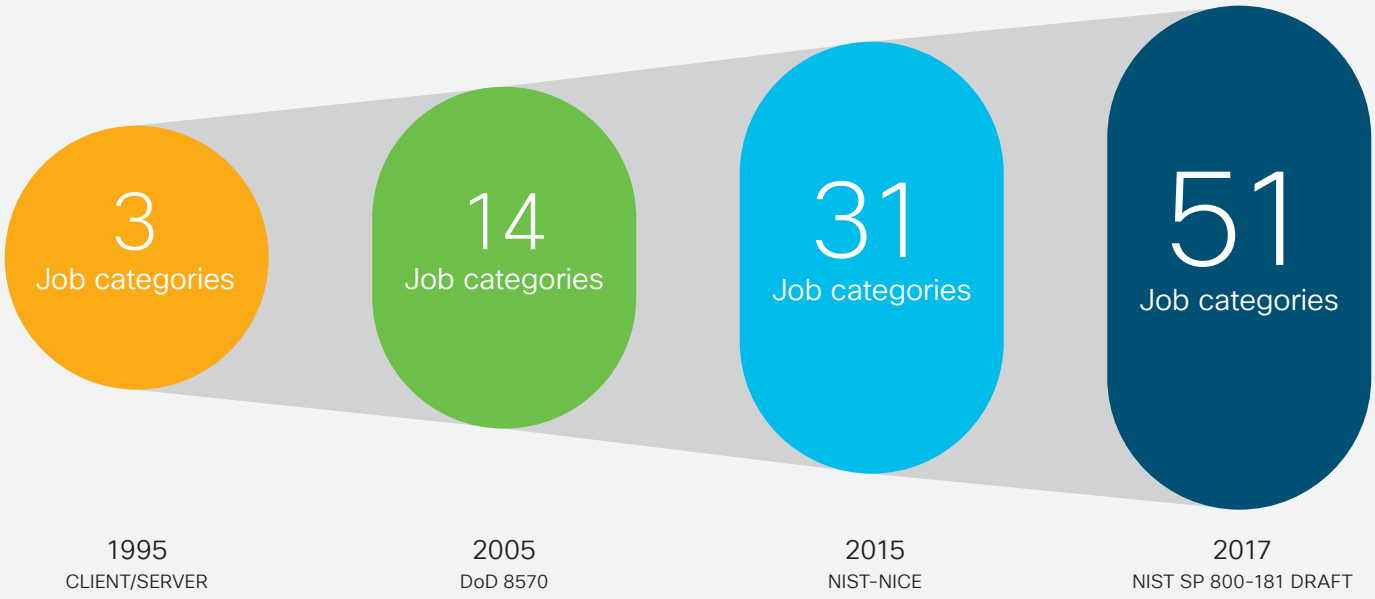
Some estimates say that certification is requested in more than 35 percent of cybersecurity jobs. And many organizations have serious expertise obstacles in that they cannot find candidates with certain skills—leaving untenable gaps on the team. These and other constraints make it more difficult to hire those who might otherwise be the best candidates.

7. DarkReading, "5 Ways the Cyber-Threat Landscape Shifted in 2016," December 19, 2016.

IT and business management roles in cybersecurity

Figure 3: Segmentation and specialization

U.S. security roles have become more complex over the years.



So, what makes a complete team? Here's how it has been addressed in the United States. We've seen an evolution in security job roles over the years. In 1995, the IT technology stack was quite simple—just three layers, each with a security component (Figure 3). Ten years later, DoD 8570 was introduced as a workforce and team organization model that many large organizations adopted. The roles were becoming more complex, with 14 job categories.

Then in 2015, the latest workforce model was introduced—the National Institute of Standards and Technology/ National Initiative for Cybersecurity Education (NIST/NICE) Model, with 31 job categories. We can see that much of the growth in security jobs has come from expanded or new segments. And a shift has occurred toward security operations (cyber ops) roles.

Now in 2017, the latest U.S. standards publication, NIST SP 800-181, will include a whopping 51 job categories. These include descriptions of nearly 1,000 tasks, nearly 100 abilities, more than 300 skills, and 600 items of knowledge. What will the future hold if positions are expanding this rapidly?

Cisco simplified the model

What this does show is that many opportunities are emerging for those who wish to enter or develop their careers in cybersecurity—and for organizations wishing to build complete teams. To plan a team structure, organizations must learn what is available and what their teams are lacking. And it may be different for each type of organization based upon its specific industry, size, objectives, regulations, and other factors.

Yet, trying to understand and explain all that information may compel everyone to run away in frustration. To make the task more manageable, Cisco has simplified the government's complex model and turned it into a quadrant framework (Figure 4, see next page). The four quadrants include the major job categories and the specific career pathways to help team members advance up the management ladder.

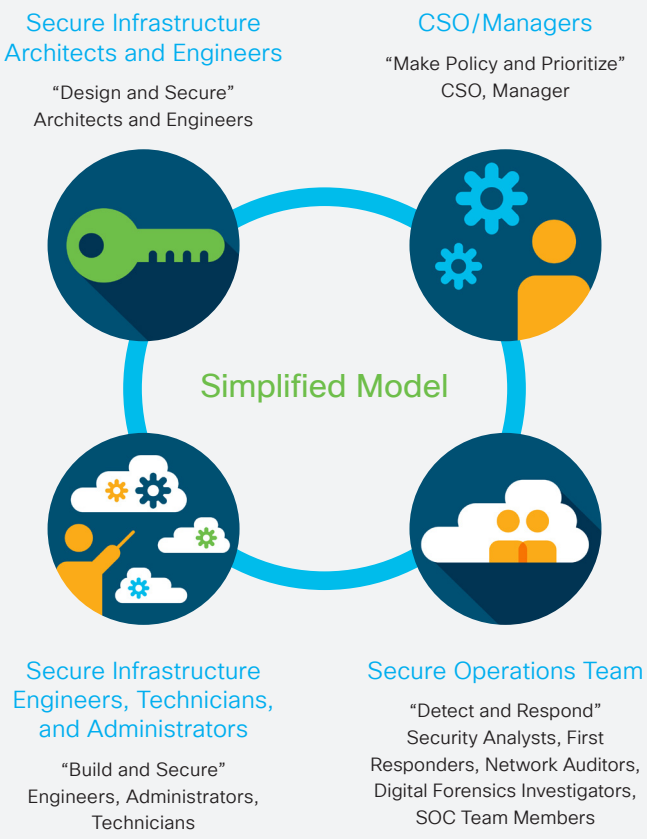
IT and business management roles in cybersecurity

These categories include:

- Chief security officers (CSOs) and managers, who make policies and prioritize risks.
- Secure infrastructure architects and engineers, who design and safeguard the system.
- Secure infrastructure engineers, technicians, and administrators, who build and secure the system.
- Security operations teams, who detect and respond to threats.

The ideal team members in each of these career pathways must have the proper attributes that will help them perform well. These include their complete list of knowledge, skills, and abilities, or KSAs, pertinent to their specific job roles.

Figure 4: Team Frameworks



Each member of the IT team should understand what positions they play and how they fit into the overall security of the organization. They also must feel integrated within an employee development program—evidence that management values their contributions and wants to help them improve their skills and performance. They want to know that they can have upward mobility in their careers if they're loyal to the organization and show promise.

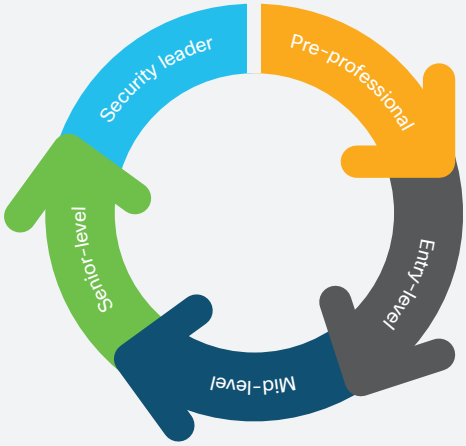
A complete team should have depth

This all can feel overwhelming. But there's good news. An organization can quickly determine what it needs. The Information Systems Security Association (ISSA) Cyber Security Career Lifecycle can be a useful guide to analyzing the depth of a team (Figure 5).

Does your team have senior-level and security leadership people in place? How are your mid-level team members developing? Are entry-level people able to take on some of the work from more experienced professionals, and are they given the opportunities to develop their skills and careers?

What team members are looking for—and what they must offer back to the team—will differ from where they fall in their career lifecycle. Having an appropriate mix of team members will optimize the effectiveness of the security team over the long term.

Figure 5: Cyber Security Career Lifecycle[8]



8. Information Systems Security Association (ISSA)

IT and business management roles in cybersecurity

Due to a global shortage of cybersecurity experts, many of these jobs are filled by hiring existing security experts away from other organizations and requiring at least five years of security experience just to apply. But is that the best way to go? Not necessarily, because the process is more complex than simply hiring a senior IT person. You must have people in training, so they can be ready to advance as they gain institutional knowledge. And do you want your senior people performing routine tasks that could be handled by a junior person?

Here's another important point. Given the global shortage of cybersecurity experts, competitors may try to poach from your team. So, how do you keep your experts in place? First, make sure they know how important they are to the organization. Provide fair compensation so they won't be tempted by a competitor's offer. Be sure that they receive training and mentoring so they understand how much they're valued. Show a clear path to advancement so your team can foresee a good future within your organization.

This team-building process may look daunting because it is impractical for some organizations to hire a complete cybersecurity team. For them, other options may be necessary:

- Some smaller organizations may hire one or two people to manage the day-to-day tasks, but they might use a larger consulting firm to handle the more critical facets.
- Larger organizations may employ teams in which each of the experts can manage a broader variety of tasks. These may be combined with the services of a consulting firm.
- Governments, healthcare institutions, large retailers, and other organizations with more attractive assets certainly will require a full-scale, in-house (and perhaps global) cybersecurity team.

Can the business and IT teams agree on priorities?

It is important for the organization's management to understand all this, but it is often a challenge to agree on how to address security issues. Why? Because management must keep its eye on business performance, operations, competitiveness, and profitability—or, in the case of nonprofits or government agencies, its budget management.

On the other hand, technology people are focused on securing and defending the system against cybercriminals. Their attention is given to patching, updating, hardening, preventing, locking down, and all the other technical aspects of keeping the organization safe.

It may appear that these two factions work in isolated worlds. But in fact, both have the same goal—helping to ensure that the organization is operating at optimal performance. They just have different ways of approaching it or even describing it. While management may balk at yet another request for IT headcount ("Didn't we just hire someone last month?"), the IT people may simply be using unfamiliar language to justify the need.

On the other hand, when IT teams are asked what they need, they may point to someone with 20 years of experience. But HR may have only enough budget for a mid-level person, or for a person with only a generalized skillset instead of a specialty. Therefore, the IT people may have to either rethink what they really need, or be better at explaining the difference between roles and the costs of alternate staffing.

> Even today, many business managers may still think they need only "a security person." But security is not just one individual, or a single role, or a single skill. A company may have a firewall expert, but in fact, that person may be trying to address many other vulnerability points.

This isn't good, especially when an organization must protect against the growing list of threats discussed earlier. This is what the IT folks must help business management understand.

IT and business management roles in cybersecurity

Communication and agreement are vital

To start that conversation, it is necessary for both the business managers and the IT managers to appreciate each other's priorities and to speak in terms that are meaningful to both sides. Here are a few sample questions that both groups could discuss. They relate to the issues introduced at the start of this paper. (A more detailed stand-alone version is available for download from the Cisco Cybersecurity Training and Certifications page. It can be printed for group discussion.):

Identifying and cataloging the assets:

- What are the organization's most and least critical assets?
- Besides physical assets, what intangible assets could be compromised?
- What types of critical data could be lost to cybercriminals?

Evaluating and prioritizing the assets:

- Which losses or damage could cause the most significant financial damage?
- What would happen if you lose control or access to critical assets?
- How would a breach affect customers, patients, clients, vendors, and others?

Uncovering potential threats and risks:

- Where are the potential security vulnerabilities in the organization?
- What systems and applications should be updated or patched?
- Does the security team have a reliable source of risk intelligence?

Staying informed about new risks:

- Does your security team have a reliable and timely source of risk intelligence so it can respond quickly?
- How is it uncovering outdated and unpatched systems and applications?
- Does it know how to patch or update systems so all security controls are working?

Understanding and documenting policies and standards:

- What types of security policies and standards are already in place?
- What standards should be developed and implemented?
- What regulations must you adhere to, and what is the cost if you do not?

Building, deploying, enforcing the processes and controls:

- What kinds of processes and controls will close security vulnerabilities?
- Can you build and deploy your own controls, or must you hire outside expertise?
- Who will monitor and update the controls?

Hiring the right people:

- Is your organization sufficiently staffed to handle the risks?
- Does your team bring a variety of skills?
- Do they have a variety of experience levels?

Continuously expanding expertise:

- Does your team have the necessary skills and certifications for tomorrow's cybersecurity issues?
- Are these skills well distributed across the team so it can provide 24-hour-a-day and holiday coverage? Are they cross-trained?
- Should you hire additional personnel or consultants who have these certifications?

IT and business management roles in cybersecurity

Building user awareness:

- How can employees be trained to recognize and communicate potential attacks?
- How often should training occur?
- Who will develop and teach the curriculum?

Planning and communicating with each other:

- Do you have a regularly reviewed set of plans to address the attack continuum?
- What's your organization's plan for what to do before, during, and after an attack?
- Does everyone know his or her role in the plan?
- Have you rehearsed your plans, and are they revised regularly?

Reviewing and evaluating:

- How often should you review and evaluate all these issues?
- Who will be charged with making sure that it happens?

The answers to these questions will continually change as threats, regulations security technologies, assets, and team members evolve. Out-of-date responses will present their own security management issues to your organization.

Note that none of this review process can happen unless the organization has at least a basic cybersecurity team in place—even if it is just one or two people. Then it must determine the most practical way to help ensure that the team is the right size and has the right expertise for the organization—whether they build that team or buy it. The important thing is to understand that IT is a critical defensive team for the organization—something worth the investment of financial and human resources.

Continuous learning supports high-performing teams

Next, both the IT and the business management teams must understand that keeping a security team's knowledge, skills, and abilities up to date takes planning and continuous education. Both individual and team skills development plans should be looked at as a natural part of maintaining an effective cybersecurity team. A team that isn't current on the latest technologies, threats, and best practices is a security incident waiting to happen. Even the finest IT team will fall behind quickly if members aren't learning new and updated skills.

Certification for cybersecurity professionals is a distinct advantage for any organization that's serious about protecting its valuable assets. Certification helps ensure that the IT team is composed of experts who can think ahead, safeguard and monitor the entire system, manage vulnerabilities, and continually improve the level of protection. Certified individuals have independent third-party proof that they have skills for a specific job, helping even nontechnical interviewers to evaluate a candidate's skills. This may be why it is estimated that more than 35 percent of cybersecurity job listings ask for a certification.

Cross-training is also necessary. When one IT resource is overloaded or when a team member is sick or on holiday, backup is required—either from cross-trained team members or from outside resources. A successful security team must be able to scale up and down. It requires people who can play a variety of positions on the team, so everyone fits together to form a single umbrella protecting the entire organization all the time.

This is also an excellent way to attract and retain those valuable cybersecurity people. Given the worldwide shortage of these certified professionals, organizations that train and value them are most likely to keep them on board.

When an organization evaluates training options for its security staff, it should look for a company whose courses are American National Standards Institute (ANSI) and International Standards Organization (ISO) compliant. Do they also offer training for a variety of professional roles? Does the training go beyond simply teaching people how to use tools? Does it also provide a broader viewpoint so they can understand the entire system? Is hands-on training offered on real working infrastructures commonly found in Fortune 500 companies? Or is the training merely theoretical? Does the training align with today's technologies and those expected in the future?

IT and business management roles in cybersecurity

Business and IT benefit from certifications

Cisco is here to help your team with a complete package of certification courses for any qualified individual who's serious about a career in cybersecurity. Training progressions are mapped out, so each learner can follow a logical pathway to fill specific specializations—or to become security managers with broad expertise.

There are more than two million IT and networking professionals in the United States alone—or 8.3 million worldwide—who could benefit from certifications, such as those that Cisco offers now and the new ones that address evolving cybersecurity issues and threats. In fact, Cisco has certified three million IT people globally.

Topics cover everything from security concepts and architecture to incident management and cleanup. IT professionals, wherever they are in their career trajectories, can earn certifications that increase their value to the organization and qualify them for advancement.

Meanwhile, business managers have a reliable resource through Cisco that helps ensure that their security teams are capable of locking down the system today and into the future. These are the priorities that both IT and business management can share as they work toward protecting organizational assets and making sure that the enterprise remains fully operational.

Tom Gilheany
Portfolio Manager, Cybersecurity Training
and Certifications, Cisco

For additional cybersecurity resources

We hope this paper has provided valuable insights. If you'd like additional resources, please visit cisco.com/go/securitytraining. You'll find:

- More detailed information about the different roles in a cybersecurity team, along with cybersecurity career planning and employee development guides
- Helpful resources, including training and certification programs for all levels and functions of a cybersecurity team
- A companion "Quick-Start Planning Tool: Checkup for Your Cybersecurity Team Strategy" to this white paper. You can print and use it as a discussion guide to help business and security management at your organization craft a sound cybersecurity team strategy.