Global Knowledge®

Expert Reference Series of White Papers

How to Build a Winning Cybersecurity Team

How to Build a Winning Cybersecurity Team

Introduction

For every organization, effective cybersecurity depends on a careful deployment of technology, processes, and people. And if you get the people right, they'll take care of the other two factors. Just like a sports teams, cybersecurity teams need to be carefully built and managed to reach optimum performance. They don't just take shape naturally.

So, how do you organize a winning cybersecurity organization? How do you divide the work? What skills do you need? This white paper will break down those questions into manageable issues and recommend solutions and best practices.

What characteristics do winning cybersecurity teams share?

Based on the insight and relationships developed over many years, Global Knowledge has developed a best practices model of a superior cybersecurity organization—bringing our research and experience to bear and validating against hundreds of organizations, from the largest to the smallest. In studying world-class cybersecurity organizations, Global Knowledge discovered several critical characteristics that successful cybersecurity organizations all seem to share. So how does an organization like yours build a winning cybersecurity team? Let’s dive in.

Step 1: Acknowledge that cybersecurity is a people problem, not a technology problem, and prioritize accordingly.

Many people assert that cybersecurity was not an issue before the advent of computers and networking. That’s true, as far as it goes. However, it is also true that every single cybersecurity attack has been initiated by a human, and every single mitigation and response was put in place by a human. Computers don’t attack computers unless told to do so by a human attacker. Systems don’t mount a defense unless configured to do so by a defender.

That's not to disparage the important breakthroughs happening in cybersecurity products today. Every week there are new announcements of advanced biometric scanners, behavioral analytics and machine-learning based systems that can detect zero-day attacks. These do improve security. However, we believe that despite all of these advanced systems, there still needs to be human engagement to make a purchase decision, deploy and integrate them into a solution. This critical piece—the human—has the largest impact on return on investment (ROI) for cybersecurity success. A firewall or intrusion prevention system that has not been properly configured by a knowledgeable human will never work as intended.

> "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." - *Bruce Schneier, Independent Security Consultant*

The single best investment a cybersecurity team can make is in themselves. That investment in knowledge, skills and abilities amplifies the value of any technology solutions they deploy. According to the Global Knowledge IT Skills and Salary Report, we've seen a global rise in IT skills gaps, especially in cybersecurity. Decision-makers are struggling to hire qualified cybersecurity talent more so than any other functional area. And the shortage of cybersecurity professionals has been trending worse in recent years.

With hiring and outsourcing a major challenge, an investment in people is more important than ever. As Steven Covey observed in his book "7 Habits of Highly effective People," you have to "Sharpen the Saw." "Sharpen the Saw" means preserving and enhancing the greatest asset you have—you. The first step in building a winning team is prioritizing people.

Step 2: Address the human element so your cybersecurity thinking can evolve ahead of the "bad guys."

As we have observed the life cycles of technology over time, there are trends in thinking about technology. Cybersecurity is no exception. It's probably not a coincidence that over time, cybersecurity thinking has evolved similarly as military thinking. At first, cybersecurity focused on a strong "perimeter defense," much like real-world forts and castles. The theory was that we can't control what goes on outside the gates. We can only build strong walls (to resist direct attacks) and closely inspect anything that comes through the gates. This type of thinking led to the successful rise of firewalls (networks) and virus checkers (computers).

Later, as attackers grew more sophisticated in camouflaging their incursions, cybersecurity evolved again. In this case, although the walls and gate inspections were still present, defenders acknowledged that if intruders did manage to gain access into the secure enclave, they could then roam freely. The response was to adopt a philosophy of "defense in depth." This model is equivalent to having guards roaming the hallways and rooms inside the castle, looking for unusual behavior from anyone. In the case of cybersecurity, this meant installing network intrusion detection systems (NIDS) on networks, and host intrusion detection systems (HIDS) on servers. This was a profound shift, from one dimensional to two dimensional thinking, and was quite successful in catching more intrusions. Now these systems not only detect, but block intrusions, making them Intrusion Prevention Systems (IPS).

The latest thinking involves the philosophy of "zero-trust" cybersecurity. This model is equivalent to locking all the rooms in the castle and only providing keys to the rooms each person needs. This lock-down model works well because, even when credentials are compromised, it limits risk exposure to minimal data and systems.
These are all strong approaches that build on each other. However, they still only operate in two dimensions (primarily technology, with a bit of policy). At Global Knowledge, we recommend a more universal approach to the problem. We believe that successful cybersecurity is a three-dimensional solution: People, Processes, and Technology. Successful cybersecurity organizations think about all three dimensions and get them right.

One dimension, as discussed previously, is technology. It's vitally important that organizations use the best technology available to address the problem of security. Organizations need to purchase and integrate best-of-breed solutions across a wide array of technologies to have the best defensive posture.

However, the second dimension, process, is even more important. It does no good to have a leading edge IPS if it's not configured and maintained properly. It can't protect systems that have not been patched and updated per best practices. It certainly can't protect against misuse of user passwords and credentials. In short, processes have to be in place before a technology solution can begin to do its job.
Finally, the most important dimension is people. Just as technology is useless without process, processes are useless without people. People need the proper knowledge, skills and abilities in order to implement and follow processes and deploy technologies. So, there are three dimensions to cybersecurity: People, Process, and Technology. The most important being the people.

Step 3: Cybersecurity is maturing into sub-specialties and professionals should develop the skills they need to "play their position."

Automobile mechanics have specialized over the years. Now there are paint shops, transmission shops, brake shops, tire shops, etc. Even if you take your car to a full-service facility or dealership, there are still specialists working there.

In the same way, cybersecurity has grown in complexity to the point that there are sub-specialties that have emerged. In our analysis of successful cybersecurity organizations, eight specific specializations have emerged over the last few years. Very large organizations have teams in each of the eight specializations. Smaller organizations with only a few cybersecurity personnel will have one person cover more than one specialization, or outsource some, or both.
The eight specializations (in no particular order) are:

- Architecture and Policy
- Data Loss Prevention
- Governance, Risk and Compliance
- Identity and Access Management
- Incident Response and Forensic Analysis
- Penetration Testing
- Secure DevOps

- Secure Software Development

Architecture and Policy

The cybersecurity architect designs and implements secure architectures and translates standards, business processes, and frameworks into internal policies. In most organizations, this is an experienced engineer, typically with many years in IT, who can make complicated tradeoff decisions. In other words, they can typically think of several ways to tackle a particular problem, and then sort through those alternatives to find the best solution. Architects are familiar with many products and protocols, and can develop functional diagrams of how applications actually work in the data center. More importantly, they are comfortable defining secure interfaces between applications and systems. The policies developed by the architects are driven by the underlying architecture they have chosen to use. Architects use frameworks to organize the architecture into manageable structures.

Data Loss Prevention (DLP)

These engineers deploy and manage security applications such as malware detection on endpoints and servers. Many modern anti-virus systems on PCs use an advanced client connected to services on the back-end to push out signature updates and the like. These engineers make sure the system stays up to date and troubleshoot negative interactions with new applications (that sometimes interfere with virus checkers). DLP personnel also manage the security of data on servers and databases, often installing and maintaining special software for permissions and logging as well. Finally, they often engage in user privacy issues and work on GDPR compliance.

Governance, Risk and Compliance (GRC)

These analysts measure and quantify risk, performs internal audits against best practices and standards, and develop plans for business continuity and disaster recovery. Risk analysis is becoming quite important because it must align with business risk. Applications and programs critical to the business need more protection than others, and it's up to these analysts to make sure the risk has been identified and mitigated properly. The GRC team typically acts as the "security auditor" and checks the work of the other seven specializations against compliance checklists such as PCI-DSS and frameworks such as the Risk Management Framework (RMF). When there are findings of non-conformance, the GRC team provides tracking and verification until they are resolved.

Identity and Access Management (IAM)

This team manages identification, authorization and permissions across all systems. Because of the proliferation of protocols and technologies (OAuth, SAML, etc.), they tend to be protocol experts across all platforms, from desktops and servers to smartphones and tablets. They also need to understand and enforce identification policies across the entire organization. This includes understanding roles and role-based access management for business processes. They also track the latest in multi-factor identification and biometrics. More importantly, this team is most directly impacted by cloud architectures, which makes the job much more complex. This function typically has less staff than the other specialties, but the most common attack is user credential compromise, so diligence is required.

Incident Response and Forensic Analysis

Even the best defenses are breached from time to time. This team runs the Security Operations Center (SOC) and does threat hunting and detection. They detect and analyze security events and correctly respond by taking appropriate action, whether that means disconnecting a machine, or simply sand-boxing a piece of software to determine if it is malware. They are also experts at forensic analysis, and can detect what an attacker did and how they did it. As a result, this team develops evidence to be used

in trial when needed, following standard chain-of-evidence rules.

Penetration Testing

This is the most commonly outsourced specialization, but many organizations still perform some internally. This team intentionally attacks systems to expose vulnerabilities and probe weaknesses. Often called the "Red Team," they attack systems and processes exactly as a black hat attacker would. Done correctly, they can expose weaknesses and vulnerabilities before the real attackers do. More importantly, they make recommendations on how to harden systems against future attack. They also perform "human engineering" tests by trying to convince users to give up sensitive information. Because of that, they are often located off-site so they aren't recognized.

Secure DevOps

This is the hands-on team that actually manages systems in the data center (or cloud). They securely install, configure, and operate systems and software—especially dedicated security products such as firewalls, intrusion detection, and even dedicated HSMs (Hardware Security Modules) to hold sensitive keys and certificates. Often, the team is called DevSecOps to signify that "security is in the middle." Even in a cloud environment, they still need to manage security processes and functions securely.

Secure Software Development

Some organizations develop software to sell as a product, while others develop their own software just to use internally. In either case, this team develops and tests applications to have minimal vulnerabilities. They typically use rigorous processes and policies regarding software architecture, and then use special tools to scan software for vulnerabilities. Application security testing can be done statically (code inspection) or dynamically (run time behavior), but most organizations need to do both.

Functional Specifications Summary

As described above, cybersecurity has matured into a complex and diverse set of functions. In a large organization, each of these eight functional areas would be represented by a separate team. In the smallest organizations, perhaps one or two individuals will try to cover as much as they can, and outsource the rest. In any case, each of these functional specializations represent different roles requiring different knowledge, skills, and abilities.

There are some natural similarities between the functional areas. For example, it's common for the Architecture and GRC roles to either work closely or be performed by the same person. Likewise, the DevSecOps, IAM and Secure Development teams often work closely together.

Finally, it's common for the Incident Response/Forensic team to do some penetration testing. It should also be noted that some of the functional specializations are often outsourced. For example, security consultants can routinely do security audits and assessments to support the GRC specialization. In addition, some companies provide penetration testing services.

Looking Forward

All of these functional specializations will continue to evolve, just as the underlying technologies will evolve as they support the evolving needs of the organization. New innovations such as cloud, IoT, machine learning, and blockchains will affect each of the eight specializations in different ways. Therefore, it's critical to the success of the cybersecurity team (and the organization as a whole) to stay on top with strong and timely training.

Like a sports team, skills must be developed for each position. Not everyone needs the same training,

but together they can be much stronger. Global Knowledge can help you get there.

Why Global Knowledge for Cybersecurity?

Global Knowledge occupies a unique position in the IT industry. As a veteran technology player, Global Knowledge has been around (much) longer than a lot of the product and services companies in the space today. We have helped professionals develop skills throughout the life cycle of many technology solutions, from routing and switching to fiber optics, and more. Over time, we've developed successful partnerships with many leading technology players.

Additionally, we train more than 300,000 students worldwide per year and benefit from the real-time feedback on the successes and failures of today's most popular technical solutions. Global Knowledge also has direct relationships with many large corporations and governments where we create and deliver customized technology classes.

Finally, Global Knowledge has developed a large community of top industry experts who develop and teach courses while also continuing to do leading edge consulting and project work in their "day jobs." With all of this taken together, we see technology and the skills required to solve problems with technology from an unmatched vantage point.

Learn More

Cybersecurity Training Courses

Cybersecurity Certification Training

Cybersecurity Glossary of Terms

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Dave Buster has over 35 years of experience as a technologist in engineering and marketing roles, bringing new technologies to market for various companies. This includes experience as a Senior Product Manager for Fiber Optic Systems, ATM Multiplexers, and Protocol Analyzers, followed by 13 years at Cisco Systems where he was Director of Product Management for Government Solutions. Dave has a B.S. in Engineering and an MBA from North Carolina State University as well as various cybersecurity certifications including Security+ and CISSP. Currently, Dave is the Global Senior Portfolio Director for Cybersecurity at Global Knowledge, an industry leader in technical education solutions.