HOW TO BUILD A SKILLED IT SECURITY TEAM IN 5 STEPS

In an era of APT and sophisticated, often state-sponsored attacks, how do you make sure that your IT Security team and your organization have the right skills to protect your most critical assets?

How are you going to guarantee that your team has the right skills to devise and implement a cyber security plan that truly addresses an ever-changing threat landscape?

This paper focuses on the critical steps every organization should take to minimize cyber security risk for the coming years.
BUDGET TRENDS

For the past few decades, corporations and governments have poured hundreds of billions of dollars into security hardware and software, only to discover that their critical infrastructure is still vulnerable to attack vectors which have been discovered and well-documented twenty or more years ago. For years, we thought that cybersecurity was a software or a hardware problem. It’s not.

It’s a people problem: people who sell you next-generation security devices; people who buy them, and ultimately, people who operate, configure, and maintain them.

According to PwC, Incidents (successful attacks) increased by 38% over the previous year (2015), confirming a trend that has been steady for the past few years: “Cyber attacks continue to escalate in frequency, severity and impact. Prevention and detection methods have proved largely ineffective against increasingly adept assaults”.

Despite common belief, technology alone is not winning over cybercrime.

Is this because corporations and governments do not invest enough into Cyber Security?

In a recent 10-K SEC filing, JP Morgan Chase, the largest bank in the US – and the sixth in the world – announced that they budgeted $600 million for cyber security in 2016. Compared to $500M in 2015 and $250M in the previous year, that it is an increase of over 100% in 2 years alone.

---


Despite this, Andy Cadel, general counsel, IP and data protection for JP Morgan Chase, told Bloomberg\(^3\) that they still feel “challenged,” so much so that they list cyber security as one of the primary risks for their investors.

Bank of America’s approach was to adapt a no-limit budget for cyber security. In the words of its CEO, Brian Moynihan, “this is the only place in the company that didn’t have a budget constraint”\(^4\).

While still under President Obama, the White House set a $19-billion budget for cyber security for FY 2017, up 35% from FY 2016\(^5\). Such figures will probably be confirmed, if not increased by the new Trump administration.

**IT Security budgets throughout the most targeted industries such as financial, retail and defense are steadily growing and will be for the foreseeable future.**

Why, if budgets are on the rise, can’t we fix, or at least minimize, the cyber security problem?

---


HOW BUDGETS ARE SPENT

According to the IDC, almost 70% of the overall IT security budget in 2016 has been spent on Managed Security Services (MSS) or Hardware / Software⁶.

A survey on more than 200 enterprise security professionals contained in Accenture’s State of Cybersecurity and Digital Trust 2016 revealed: “Cybersecurity teams are struggling, with 42 percent of respondents believing that while they have enough budget for security technology, they need additional budget for hiring security talent and training.”⁷

This is in-line with other research⁸ ⁹ that project a shortage of between 1.5 and 2 million cyber security professionals by 2019, making skilled IT security professionals highly sought-after and hard to find.

In the words of Robert Herjavec, Founder and CEO of Herjavec Group, a Managed Security Services Provider: “Unfortunately the pipeline of security talent isn’t where it needs to be to help curb the cybercrime epidemic.”

He goes on to say...

“Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats.”

---

CHANGES IN THE THREAT LANDSCAPE

The threat landscape is continuously evolving.

Large organizations are now facing attacks at an unprecedented level of sophistication. State-sponsored attacks, cyber-espionage from competition and APTs in general, all leverage 0-days, stealthy techniques, and “slow-cooked” exfiltration techniques, that make intrusion detection a matter of months, if not years.

Time to detect, and time to remediate are two of the most important cyber security metrics and are worsening as a result.
According to a Deloitte analysis of breaches in financial industry organizations, 88% of the time, attackers successfully breach a company in a matter of hours. ¹⁰

While in 38% of the cases, it takes months or even years for that organization to discover the incident!

**A BLENDED APPROACH TO SECURITY**

Organizations need to have skills, ranging from security awareness to the most advanced hacking techniques, to be prepared to combat sophisticated attacks.

By having a workforce with practical skills on cyber security, an organization will be able to:

- Properly evaluate risk based on facts rather than on next-generation UTM marketing collaterals.
- Perform internal audits that can mimic advanced persistent threats and can confidentially uncover security pitfalls within the organization.
- Hunt for adversaries to drastically decrease the discovery time and the chances that digital information gets exfiltrated.
- Drastically decrease the effectiveness of social engineering and spear phishing attacks.

A skilled IT Security team helps: reduce *time to detect, time to resolve* and *risk per host*. This translates in an improved security posture.

---

5 STEPS TO A SKILLED IT SECURITY TEAM

IT Security has such a vast knowledge domain that building in-house skills might look overwhelming, time consuming, and expensive.

The following are 5 steps an organization can take to drastically improve their security posture while maintaining efficiency and controlling training costs.

1. Define Essential Team Roles

To begin with, the IT Security team should have a clear separation of responsibilities, and each member should have a clear career path, matched with proper training.

Whether the team is large or small, the following logical separation helps in defining roles and required skills:

- **The Security Engineering Team** is involved at design time, to install, configure, and operate security software and hardware. This team is also responsible for hardening systems and applying patches.

- **The Proactive or Red Team** is involved with proactive auditing and penetration testing of systems, simulating sophisticated external and internal adversaries with the goal of uncovering vulnerabilities and testing defenses.

- **The Blue Team** is involved with the monitoring, response, investigation, and analysis of security incidents. Also known as the **Intrusion Detection and Response Team**, it often becomes an extension to the engineering team in undertaking defensive roles, while benefiting from the presence of the Red team, and improving day-by-day operation with the Red Team’s input.

- **Management** defines strategic goals for the entire team, based on the organization’s IT Security needs and objectives. This strategy should translate into security policies, hiring plans, training plans, budgeting, and performance review.

Having a clear logical segmentation of the IT Security team is the first step towards building competencies that are relevant to the roles of each member.
Lay Common Ground (Practical) Skills

Regardless of the roles covered in your IT Security team, there are certain skills that are relevant across the board. Without proper practical training in those skills, any training effort would be ineffective.

A practical understanding of today’s threats is critical not only to members of the Red Team but also to:

- Blue Team / security engineers
- Security managers

Security engineers and members of the Blue Team deal with cyber threats every day. Their understanding of the practical aspects of cyber threats is imperative to properly and readily respond and remediate.

Security managers are responsible for planning security initiatives based on facts rather than vendors’ marketing. This is done by relying on their own team’s advanced practical skills. It gives them the skills to better assess, evaluate, and make decisions.

Practical training for everyone involved in defensive and offensive roles within an IT Security team should include the following areas:

- Network attack techniques
- Web application and Mobile attack techniques
- Modern malware (e.g. ransomware) analysis
- Covert channels and other APT techniques
Define Training Paths

IT Security requires a high degree of specialization. There is no single training that can make anyone a professional in any subject. But there are training paths, a series of time-tested training courses, that can make someone with the right foundation skills, a hands-on proficient professional.

Very advanced roles such as Penetration Tester, Threat Hunter or Digital Forensic Analyst require a series of competencies that cannot be built in a 5-day classroom training.

The following is a non-exhaustive map of competencies that each role in an IT Security team should have.
Map of Competencies for IT Security Professionals

**Roles**

- **Red Team**
  - Vulnerability assessment
  - Network Pentesting
  - Web App Pentesting
  - Mobile Pentesting
  - Advanced Exploitation
  - Covert techniques
  - Defense Evasion
  - Exfiltration
  - Persistence and lateral movement
  - Physical security
  - Social Engineering

- **Blue Team**
  - Monitoring
  - Intrusion detection
  - Incident Response
  - Digital Forensics
  - Malware analysis
  - Threat Intelligence
  - Threat Hunting

- **Security Engineer**
  - Secure network design
  - OS Hardening
  - Network devices hardening
  - Patch management

**Required Hands On Skills**

**IT Security Fundamentals**
- Threat analysis and classification
- Basics of auditing and penetration testing
- Vulnerability assessment
- Attack vectors terminology
- Risk assessment

**Foundation Skills**
- Networking protocols
- Operating systems: Windows and Linux Programming
By using the above map, a security manager can perform a skills gap analysis and set training goals for each of their members on a mid-term (1 to 3 years) basis.

Go for Practical Training

Once the security manager has devised a solid training plan for their team, which training is the next decision. This decision is of vital importance.

The goal is to have the team proficient at work as soon as possible – so, as in any other business decision, it boils down to a risk/benefit analysis:

✓ How soon can the team be ready to apply the learned techniques at work?
✓ How effective is the training delivery method?
✓ How much does it cost the company?

Practical training based on sophisticated virtual labs immerses the student in many different real-world situations in which a cyber security problem should be solved.
These “situations”, also called virtual lab scenarios, are specifically built by subject matter experts to effectively transfer hard-earned experience in a matter of hours.

For years, military and defense organizations have benefited from such technology in their cyber-ranges. This technology is available today for organizations of all sizes and at a reasonable cost.

Moreover, practical training that is also self-paced is the best solution, when the organization wants to immediately acquire internal skills, while having the flexibility of allocating training time when it makes more sense to the company.

Virtual labs that are isolated, realistic and on-demand provide the best training experience.

5 Measure your team’s practical performances

As a security manager or team leader, measuring performances helps build the ROTI (Return on Training Investment) and obtain valuable feedback on where your team needs to focus the most.

But how do successful managers measure competencies?

How can one be 100% sure of the skills effectively acquired by attending a given training – especially if it’s online/self-paced?
The answer is: Practical certification programs that assess the practical skills acquired by the student in that knowledge domain.

IT Security, just like any other extremely technical field, is a domain where practical proficiencies cannot be assessed through multiple choice exams, because they do not capture how the IT Security professional will behave in a real, often hectic, situation of a cyber-attack.

The industry and its old-fashioned certification schemes are now shifting towards practical assessments, where candidates give proof of their abilities through obtaining certifications, that not only bring value to the company, but also the individual.
We are eLearnSecurity.

Based in Santa Clara, California and with offices in Pisa, Italy and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training. Best of breed virtualization technology, in-house projects such as Coliseu Web Application Security Framework and Hera Network Security Lab, have changed the way students learn and practice new skills.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com