The modern world takes place in a largely digital space. Underneath the physical assets that drive our businesses are mountains of data and personal information. The digitizing of information has had a major impact on the business world, creating large, complicated systems. At the foundation of it all is the ability to create a secure network infrastructure; without proper security measures and controls in place, it is impossible for an organization to move forward with confidence. Security is at the foundation of an organization’s ability to provide reliable, scalable services and protect personal information. Unfortunately, the constant movement of data opens the door to the threat of cyberattacks.
Widening Gaps in Cybersecurity Skillsets

Headlines announcing breaches and news coverage focusing on the protections of personal information have skyrocketed. As a result, we are seeing a shift in how companies approach cybersecurity.

It’s no longer a problem just for the IT department, but for businesses as a whole. Not only are CIOs and other technology executives making cybersecurity a priority, but leaders in business and marketing are seeing the importance of increased protections as well. World-wide governments are even working to put stricter sanctions in place, such as the GDPR (General Data Protection Regulation which governs how companies handle personal information for citizens of the European Union), to ensure people have more control over the use of their personal data.

However, despite the need for improved cybersecurity measures, businesses are still faced with skills gaps in cybersecurity professionals. Even fewer companies use meaningful metrics for justifying training. Companies are often content putting teams and tools in place, assuming cybersecurity will happen as a natural course of those efforts. This fallacy leaves no room for training, development, or investment into the staff who protect the company’s network and flow of information. As it turns out, only 21 percent of businesses “feel that their current level of security is completely satisfactory.” This allows knowledge gaps to form and widen over time, exposing companies to unnecessary vulnerabilities.

Companies can no longer afford to rely on third parties or anti-virus software to ward off attacks. Instead, businesses need real procedures to prevent attacks that are driven by metrics and proven methodology. Cybersecurity authority, Tim Crothers, observes that “Adversaries to cyber are constantly evolving, continually iterating. As a result of that pattern, we have to adopt a similar pattern of behavior.”

—Tim Crothers
How Skills Gaps Develop in Organizations

Businesses function on multiple levels. In complex work environments, leaders make decisions to propel the business forward. There is a constant push to bring in more customers and revenue. When leaders are faced with the allocation of resources, they analyze the benefit to the company. When evaluating cybersecurity, leaders are often faced with questions such as:

- How does cybersecurity help the bottom line?
- How much will the costs of implementing security affect our operating margin?
- Why should we invest more in cybersecurity if it doesn’t help generate revenue?
- How much will implementing security controls inhibit our ability to do business?

Decision makers want hard numbers and metrics which illustrate the value of an investment. However, because it is difficult to quantify the value of cybersecurity, decision makers are often hesitant to allocate a large investment to that section of the business. Benjamin Sondgeroth, CISSP, states, “The most important metric that we can show management is how security measures bring on or help retain a particular customer. If you can generate money, it’s a step above the standard security work.”

It becomes a situation where cybersecurity professionals are not keeping up with the training needed to combat sophisticated cyberattacks because they aren’t able to illustrate a business benefit. As a result, professionals lack vital training and the company becomes subject to gaps in security.

“The most important metric that we can show management is how security measures bring on or help retain a particular customer. If you can generate money, it’s a step above the standard security work.”

—Benjamin Sondgeroth, CISSP
The Need for Cybersecurity

As with any security risk, companies take precautions to protect their physical and intellectual assets, prevent theft, and minimize loss. Physical security has challenges, such as:

- Have you secured your points of entry?
- Do you have protocols for entry and exit?
- Are assets protected by surveillance?

But the threats posed by digital attacks can be difficult to make visible to executives. The situation becomes more of a denial discussion involving questions such as, “Why do we need to invest more into cybersecurity?” and “If a breach hasn’t occurred, aren’t we already doing all we need to protect ourselves?” As a result, businesses often fail to see the benefit of upskilling their cybersecurity professionals. Then, training lacks and organizations get hacked. The truth is that organizations actually save money by investing in cybersecurity. It’s just a question of convincing organizations to invest properly.
The Case for Consistent Training and Cybersecurity Certifications

Cybersecurity is vital for any organization that handles digital information. In fact, much of what drives customers to do business with certain organizations directly involves trust. Consumers want to know that their investment and information is protected. According to a 2016 FireEye report,

- **52 percent** of consumers would consider paying more for the same products or services from a provider with better data security.
- **78 percent** of consumers are cautious of organizations’ abilities to keep data safe.
- **52 percent** of consumers said security is an important or main consideration when buying products and services.

If a breach occurs, consumers lose trust in a brand and take their business elsewhere. The same study states that, “75 percent of consumers stated they were likely to stop purchasing from a company if a data breach was found to be linked to the board failing to prioritize cyber security.” Breaches also make it more difficult to bring in new sales because consumers become wary of brands that have a history of breached information. In order to acquire new sales and encourage customer retention, businesses need to illustrate that they are taking action to protect customers from a breach.
As quickly as solutions are being devised for cyberattacks, new attacks are being formulated. As a result, cybersecurity professionals need to be constantly evolving as well. However, without clear metrics to illustrate how businesses benefit from the investment, it can be difficult to convince organizations that consistent training is needed. In order to train teams properly and upskill them to meet these threats, companies need the backing of their leaders.

How to Communicate the Value of Upskilling to Your Organization’s Leaders

In a large organization, departments often vie for their allotment of company resources. Tech teams are no different. To get the support to train cyberteams, decision makers need to recognize the value of the investment. But without showing how cybersecurity directly impacts the bottom line, it may be difficult to get the buy-in you need.

Often, it may be easier to get buy-in for tools such as preventative software or firewalls to help prevent breaches. Because software tools such as intrusion detection systems or Security Information Event Monitoring (SIEM) platforms show a quantifiable benefit (i.e. 350 blocked attempts), it can be easier to gain support for this type of security control. But, without the right professionals, those tools won’t yield the results you are seeking. Tim Crothers offers this analogy: “Imagine a hammer. If you give it to a master craftsman, you will get very different results than if you offer it to an amateur. The results will be very different even with the same tool.” Without the proper training for upskilling cybersecurity professionals, controls that you put in place, you won’t be using the tools you have properly.
Metrics for Success: Is Your Investment in Cybersecurity Training Paying Off?

So how do you show the value of upskilling your cybersecurity team?

The solution involves a two-pronged approach.

1. Illustrate how upskilling your cybersecurity team actually contributes to achieving business goals.

2. Close the communication gap between tech teams and leaders to ensure decision makers are more informed.

Start by gathering the appropriate information.

Using Metrics to Illustrate the Value of Cybersecurity

How can you measure the value of a cybersecurity team? There are certain indicators you can look at to help determine the effectiveness of your efforts.

**Dwell time:**

Dwell time starts when a threat has invaded a system. It is the amount of time it takes to determine a breach has occurred. This factor is the overall time a threat has access to information without being detected. A large advantage can be gained by hackers if those attacks go unnoticed. The longer they have access, the more damage can occur. One method for illustrating value to leaders involves showing improvements in incident identification. According to the 2017 Cost of Data Breach Study by the Ponemon Institute, “The more records lost, the higher the cost of the data breach.”

**Incident response time:**

Once an incident has been discovered, how long does it take before a team is able to respond to the threat? The amount of time it takes to respond gives an attacker more time on your network to possibly retrieve sensitive information. Improving your response time is measurable and can help communicate improvement to leaders.
**Containment Time:**
Containment time refers to the amount of time it takes a cyber team to eliminate the threat. The less time an attacker has access to your network, the less opportunity exists for loss of data. There is a direct correlation between losses and containment time. Ponemon also reports that, “The faster the data breach can be identified and contained, the lower the costs.”

**Exposure Time:**
This is the total amount of time a threat has access to a system. This begins with the launch of an attack and is complete when the threat is completely removed from a system.

“The faster the data breach can be identified and contained, the lower the costs.”

In addition to these factors, the cost of a breach can also be very telling when trying to bring your leaders on board. Here are some of the major breaches and the resulting costs:

- **Target** underwent a breach in 2013-14 which compromised the cardholder information of 110 million consumers. The cost of the breach was an estimated $162 million.
- **Anthem** faced a data breach of 78 million users in 2015 and eventually settled the matter for $115 million.\(^4\)
- **Home Depot** experienced a breach of 56 million users’ credit and debit card information. The breach cost the company an estimated $161 million.

While it may be difficult to show the benefit of cybersecurity, the numbers associated with a breach speak loud and clear and can set companies back millions of dollars.

When viewed from the perspective of metrics and the cost of a breach, it is easier to calculate value in terms of prevention. By preventing costly attacks, cyberteams are effectively reducing losses and increasing revenue by encouraging trust. Preventing attacks is essential in gaining and keeping the trust of consumers. Building that trust leads to higher customer retention and an increase in new consumers.
While a breach isn’t ideal, how a company handles the situation can certainly speak volumes. For example, Target’s handling of their breach resulted in a discount for customers, free credit monitoring (for one year) for affected cardholders, adoption of two-factor authentication cards and an overhaul of their security systems to prevent a future breach from occurring again. Today, the company proactively approaches cybersecurity and encourages transparency to bolster the trust of their consumers.5

Once you have gathered the appropriate data, it’s important to translate it from tech speak to business speak.

Tech teams are inherently separate from other departments in an organization. Similar to national divides, tech teams are partitioned off by a language barrier of sorts. The second step to gaining buy-in involves communication. Tech teams need to speak the language of their leaders, illustrating value in business terms, rather than tech phrasing.
Ian Trump, CTO for Octopi Managed Services, Inc. in the United Kingdom, recognized the need for improved communication between tech teams and decision makers:

“If you talk about downtime, remediation costs, unanticipated costs across the business... and the potential for regulatory action from a cybersecurity incident you’re missing the point. Talk instead about how all your cyber stuff... will ensure the success of the company’s goals, how your team can get ready for the current and future threats, tell them about how your security program will drive competitive advantage... For IT in general, if you want a secure environment for the business, you need folks that know how to do that in a professional, business-friendly manner.”

—Ian Trump, CTO

Ultimately, attempts to recruit leadership to support closing critical skills gaps will be more successful when put in terms that make real business sense. Once you have buy-in, you can start the process of upskilling.
The Value of Technical Certifications in Upskilling

Certifications are valuable tools for filling skills gaps and for ensuring professionals on your team are continuing to develop valuable, real-world expertise. Unlike academic courses, individual team members can choose to become certified in the areas that are most applicable without relearning material they have already mastered. Certifications also have the added advantage of allowing companies to handpick the skills that are most important for individual business models.

Regardless of the unique circumstances that impact individual businesses, cyber training is valuable in any organization. Ian Trump said, “If you want employees and the business to be secure, you need to incentivise that through professional development. Security across an organization to reduce risk does not happen magically. It requires investment, execution and commitment across all employees.”

Create a learning culture with continued training and access to technical certifications. You will reap the benefits of informed, highly trained IT professionals who have the skills needed to combat attacks in today’s ever-changing digital landscape.

“If you want employees and the business to be secure, you need to incentivise that through professional development. Security across an organization to reduce risk does not happen magically. It requires investment, execution and commitment across all employees.”

—Ian Trump, CTO
References


