CLEARNETWORK

WHITE PAPER

An Open Letter to Chief Financial Officers:

The Last Line of Cyber Defense

A call to action.

Technology experts, information security professionals, systems and network engineers, and IT Directors. One thing that they all have in common when it comes to their organization's cybersecurity posture; they need your stamp of approval. As a financial officer of an organization, you hold arguably one of the most critical keys to cyber-success. When rubber meets the road, your approvals and denials for cybersecurity related funds can create the forecast for the organization's cybersecurity resiliency. If you have a Chief Information Security Officer (CISO), this can help you in making both informed and economical decisions when it comes to your cybersecurity. However, without an internal cybersecurity champion to assist, you are often left with very difficult decisions to make that could dictate the fate of your organization. You must be informed. You must make decisions. You must recognize the risks of cyber warfare.

According to the 2018 Verizon Data Breach Report, 73% of breaches were perpetrated by outsiders, 28% involved internal actors, 2% involved partners, 2% featured multiple parties, and **58% of the victims were categorized as small businesses** (TemplarBit.com). Small businesses are under siege and cyber-attackers view them as easy prey with high returns on investments.

Defining your organization's value.

As cybersecurity experts and evangelists, our community measures organizational cybersecurity postures based on the CIA Triad. Confidentiality, Integrity, and Availability. Therefore, our methodologies are rather simple to measure and implement, if predicated on these foundational principles. However, as a financial expert you must calculate the risks and benefits of your spending. Outside of EBIT, COGS, MRR, and other financial analysis metrics, cybersecurity spending must be carefully examined from a new perspective. By answering these three questions, you will be better equipped to make educated and calculated decisions about your cybersecurity spending.

1. What is your data and what is the value?

As a business, your data means something and has some level of significance. Whether your valuable data consists of intellectual property, customer information, credit card numbers, health data, financial data, military or defense secrets, or even internal processes that give your company a competitive edge, it is critical that you define what it is worth. Define how much the data influences the profitability of the organization, what it would cost if the data were lost, stolen, or destroyed, and what it would cost to start over with no data. Determine what this data could be worth to attackers **and competitors.**

2. What is the value of your uptime?

What does it cost for every hour that your business is not able to operate? In most ransomware attacks, this is one of the first questions that is addressed since this type of attack can cripple an organization. Imagine that you cannot manufacture goods, treat patients, accept payments, communicate with customers, ship products, or operate your website. Define what this value is per hour and add the cost for an incident response team to recover your organization at a rate of $400 - $700 per hour. The costs can be staggering and 3-7 business days without operations can spell the end of most organizations

3. What is the value of your organizations' reputation?

Beyond the costs of a breach, systems lost, recovery time, notification to patients and customers; what does this mean for your reputation. Organizations build their brands for decades, only to have them tarnished in a single moment. This is, by far, one of the most destructive and longest lasting adverse effects of a data breach. While Equifax, Marriot, Home Depot, and Target are all shining examples of reputation damage, small businesses are not as resilient. The big names hold so much market share that customers have limited choices and usually rebound to purchasing again. However, small and medium businesses do not have the luxury of losing the trust of their clients and partners. Your brand and reputation are everything. **Protect it!**

The cost of a breach

A recent undisclosed breach that was responded to by the author of this article serves as a prime example of what a breach can cost a business. A mid-level manufacturing company was hit with a cyber-attack, involving ransomware, unauthorized wire transfers, and data theft.

The attackers had breached the company for 6 months prior to discovery…

The costs were as follows:

1. Unauthorized Wire Transfers: $198,000
2. Ransomware Payments: $200,000
3. Incident Response Costs: $40,000
4. Downtime: $2.4 Million

The victim company lost approximately $10,000 for every hour that they could not manufacture and ship their products. **The downtime lasted nearly 10 full days before systems could be recovered completely.**

The total cost of the breach was almost $2.5 Million USD. However, this does not account for the tarnished relationships with their partners and customers. During the breach, customer and partner information was stolen. Trade secrets were lifted, and the attackers used the company's legitimate communication channels to send malware and phishing attacks to partner companies and customers. The aftermath of this breach was extremely damaging, and this is a common theme among small to medium businesses that are attacked.

Where to intelligently spend

If you believe that antivirus and firewalls are the way to go, the manufacturing company above did as well. This is not an uncommon pattern among organizations to assume cyber-defense equates to firewalls and antivirus. However, they are among the most ineffective pieces of a layered defense. **You need a security operations center and professional team.** Luckily, you do not have to build one. Managed Security Solutions Providers (MSSP's) have solutions to help organizations just like yours. A buzzword that you may or may not have heard is SIEM. This stands for "Security Information and Event Management". This is the essential and most comprehensive defense and detection platform on the market today. 10 years ago, only Forbes Top 50 companies and national governments could afford such ground-breaking tech. However, in 2019 **you can afford it as well; and you should.**

An MSSP Security Operations Center will:

- Collect all logs from all systems and devices within your network.
- Alert **you** when potential intrusions are occurring (Not 6 months later).
- Scan your systems for vulnerabilities that attackers can potentially exploit to gain control over your systems and data.
- Alert **you** when an attacker may be probing your network.
- Alert **you** when an attacker or **malicious insider** is stealing your sensitive data.
- Alert **you** when and if malware, viruses, trojans, or other malicious code enters the boundaries of your network and guide incident responders **quickly**.
- Alert **you** when accounts are compromised.
- Track and alert on anomalies. Most malware slips past antivirus and firewalls with ease. Detection of abnormal code activities is critical.
- Give you metrics and tracking compliance for **GDPR, HIPAA, SOC, ISO, PCI-DSS, DFARS (NIST 800-171), NIST/FedRAMP, SOX, GLBA, NERC-CIP, NYS-DFS (23 NYCRR 500), and more.**
- Detect malicious insider activities.
- ***Give you peace of mind***

By implementing a Security Operations Center through an MSSP using a SIEM, you are performing the due diligence required to keep your cyber-adversaries at-bay. If the breached manufacturing company had engaged with an MSSP and implemented a SIEM solution, the 6-month cyber-attack could have been detected and thwarted while still in its' infancy, prior to attackers compromising even the first system.

One of the major benefits of choosing an MSSP and SIEM combination is that you do not need to hire an internal security team, train them, deploy the solution, and retain the security team members. You always have cybersecurity sentries watching your network, **day and night**. Taking on such a defensive operation internally is costly, time consuming, and requires advanced knowledge of cyber-defense. Leave this to the experts and **start the discussion today**.

In closing

The information security community is inundated with cyber-attacks. **The unemployment rate for cybersecurity is 0%**. The demand for cybersecurity professionals is approximately 6 million globally as of 2019 and the median salary of these professionals is tagged around $90,000 (SecurityBoulevard). There is a major catalyst behind these figures and is a direct result of the cyberwar that we are in.

No matter the size of your organization, business model, revenue, industry, or digital footprint; you are under attack. By reading the news, speaking with colleagues, business partners, and your IT-team; you likely believe that this problem is growing exponentially, and it is not a matter of **if;** but **when.** Deciding how to spend on cybersecurity can be difficult. However, the potential costs of not spending proactively today can eclipse such hesitation. Be informed, be aware, and stay vigilant.

As a financial authority of your organization, you hold the power to protect the livelihoods of your colleagues. Your decisions to bolster the defenses can be the only factor sitting between the continued success of your organization and a
potential cyber-disaster. Investing in your cybersecurity today can give you a competitive edge, proactive posture, security-conscious culture, and mitigate future financial risks. Forecasting cyber-defense spending is achievable. However, predicting reactive costs for incident response and recovery is nearly impossible.

The information security community implores you to recognize the criticality of your position in the war against cyber-attackers. Together, we can win the fight to keep our businesses and data confidential, available, and valuable.