

**TIP Publication Date**

April 9, 2015

# You Need a Thorough Cybersecurity Strategy

## And You Need it Now!

Already in 2015 we have seen myriad reports of data theft, security breaches, and other such cases of where good intentions go very bad. This year is heating up the Cybersecurity industry, both for the good guys (those you authorize to store and access your data) and the bad guys (Cybercriminals, those lacking your consent whom can profit from your data). Never before have Cybercriminals had such a sophisticated and robust set of resources available to them; the marketplace is a booming industry with all of the features, convenience, and polish that you see in any other professional service offering or packaged application.

You can quite easily rent-an-attack by the hour with high confidence in the effectiveness and quality of service being offered, minimal risk of being caught, and you can even get access to a customer service representative in the event you run into issues while plotting or carrying out your attack! The truth is that as with any product or service exchanged for money, reliability, popularity, legitimacy, and profitability are achieved when you deliver on your promise and capability. If it were expensive, risky, or unpredictable to launch a DDoS attack against a rival, there wouldn't be a long term sustainable market for the perpetrator. The 'crime-as-a-service' model is rapidly maturing quite simply because of the high profit and low risk nature of the industry.

With the bad guys getting better by the day and the good guys putting more resources into defenses, what we are dealing with now is likely just the tip of the iceberg. It is no longer enough to rely on your hardware and software vendors to write better code and provide better patching.

The chief strategy that organizations tend to deploy is called "Defense in Depth" and is intended to employ multiple layers of mechanisms to mitigate and prevent the magnitude of a given cyberattack.

## **Background**

“Defense in Depth”, or its cousin, “Defense in Breadth”, capitalizes on the wartime strategy of putting up multiple lines of differing defense mechanisms aimed at progressively weakening an attack before it gets to what you are trying to protect, such as:

- A crocodile filled moat around your castle (a fire-breathing dragon wouldn’t hurt either)
- Deadfall pits, followed by people in trees throwing rocks, followed by spearmen sentried outside of your fort
- Cannons, musketeers, and mounted spearmen surrounding your city
- The Army, Navy, Air Force, Marines, and Coast Guard protecting the United States of America and its interests

While these strategies have provided a framework and reference point, we must pivot from the physical world to the digital world to better fortify protection of our intangible goods, or data.

Classically, Defense in Depth leverages three fundamental categorizations – People, Process, and Technology.

The “People” category includes:

- Roles/Responsibilities – Who is authorized to perform what function of the business?
- Physical Security – Who has access to what assets?
- Employees, Clients, and Vendors – Are you protected from in insider attack?
- Social Engineering – Are your employees being duped into increasing your risk?

The “Process”, or Operations, category includes:

- Policies – Published standards governing behavior
- Patching/Updates – Keeping your systems up to date
- Recovery – How do we respond to an outage/attack/breach?
- Monitoring/Event Logging – Paying close attention to what is happening
- Assessment/Audit – Regular evaluation of the control mechanisms in place

And the “Technology” category factors in things like:

- Cloud – Off-premise services that mitigate trouble before it reaches your network
- Infrastructure – Protection throughout the labyrinth of physical and logical connectivity within the company’s network (Firewalls, Load Balances, IDS)
- Endpoints – Individual user and server computers, mobile devices, and VPN connections
- Applications – Code reviews, security patching
- Data Encryption – Making sure your data is secure while at rest and in-flight

These areas are intended to address all facets of protecting organizations' digital property and we can conclude by experience and practice that these are generally correct and appropriate areas of focus for most organizations.

The importance of the Defense in Depth strategy is that it creates redundant, complementary, and independent mechanisms that individually address a specific weakness while collectively providing a blanket of protection that is more effective or reliable than the sum of its parts.

---

*"The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon." – U.S.NRC*

---

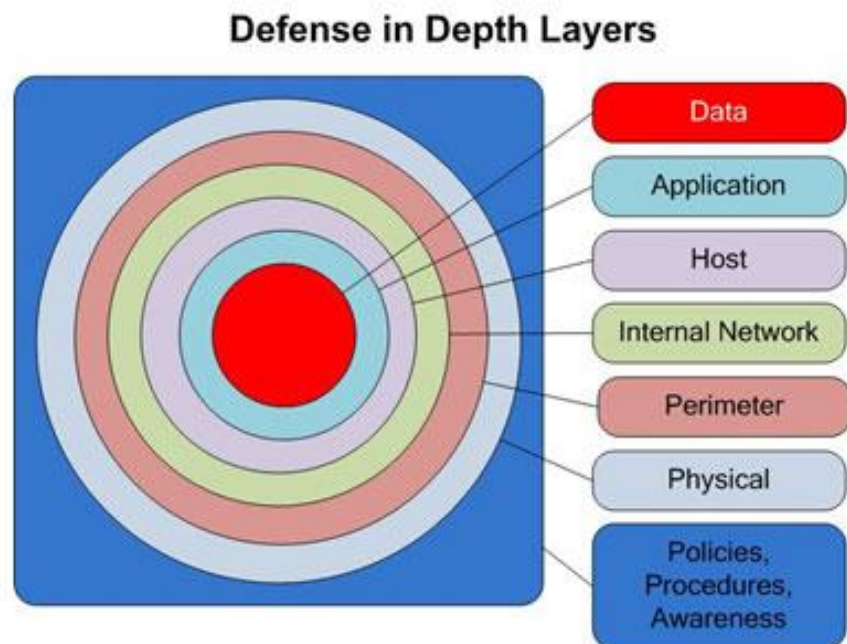
An appropriate analogy here would be the security of your home. To protect the front and back doors, you may install a dead-bolt and floodlights as a deterrent; locks installed on windows protect that point of entry. To keep the likes of Santa out of your house, you could seal off your chimney. Lastly, you may subscribe to a home security service which may leverage motion sensors and alarms in the event a window gets broken. It is also important to balance your defenses – meaning, there would be relatively no benefit to installing a second dead-bolt on your doors if you haven't latched your windows. This latter concept is known as "Balanced Defense in Depth".

As we are well aware, many homes with all of these layers of protection still get broken into and thieves remove valuables from within the home with relative ease. Similarly, in the world of data security, not only must we do what we can to keep the cybercriminals out, we need to take comparable measures to keep the data from getting out of the network (exfiltration) in the event the bad guys do get in. This example illustrates that you effectively need to double your protection, inbound and outbound.

In light of the daunting list of holes you have to plug, it still isn't enough. In fact, it is never enough. A simple fact is that you can never be fully secure as long as you have interconnected computing resources. The lists of items you read about are akin to the list of points within a house that should be addressed – we protect what we know. Doors, windows, the chimney equate to network ingress/egress points, endpoints, and the infrastructure. In a rather extreme example, it is possible for someone to tunnel in under your home and bypass the areas you've protected. This extreme example becomes a trivial one in the world of Cybersecurity protection as the list of entry points is virtually limitless given the quantity of devices, applications, software versions, and the human component (i.e. if a fully authorized admin decides to be

complicit in a breach, there isn't much you could have done to protect against that aside from your policies, procedures, technology, and monitoring).

A zero-day exploit is one that is not publically known, or newly identified to which there is no patch. The window of opportunity to leverage these vulnerabilities can last days, weeks, months, or {gasp!} years. For example, systems still running on Windows XP will remain vulnerable to any zero day exploit indefinitely, because Microsoft has discontinued support and will no longer provide patches. (Note: There are exceptions; for instance, the recent discovery of the FREAK vulnerability was so egregious and widespread that Microsoft developed a patch to protect the millions of remaining XP users.) The bad guys may not expose/act upon a zero-day exploit for several years, all the while using the opportunity to lay the groundwork and propagate agents before the hole is discovered. As we've learned, we can only block entry points that we know about.



Do not lose hope! There are many things you and your organization can do to better position your defenses. Even though you will never be fully secure without an ongoing effort, having the proper strategy in place can mean the difference between being tomorrow's headline and continuing your profitable growth.

### **Develop a Strategy**

Using Trexin's People, Process, and Technology [list](#) discussed on page 2 as a starting point, begin to build (or further expand) your different layers of defense. If your organization lacks proper and thorough documentation of your IT and data assets, prioritize that right now! In fact, creating a dedicated security role or team is crucial to your future security. The size of this

function should be proportionate to your size and type of company. You need experts here, with deep understanding, experience, and ability.

Build a foundation and get really good at covering the basics first. It's very cool to spend a boatload on infrastructure and play with new toys, but if you aren't properly performing monitoring tasks, audits, and log reviews, you've actually put yourself in a worse position. If you don't have the staff on hand, there is a long line of vendors more than willing to help you with any aspect of your strategy. Leveraging a third party expert is often a great opportunity to fast track the learning curve and increase the skillset of your internal staff while quickly remediating deficiencies in your environment.

Another critical ingredient to your foundation is understanding your lines of business and determining legitimate vs. illegitimate activity. For instance, an employee sending an e-mail with their own SSN to enroll in benefits may always be considered proper data exfiltration, but there are likely only a handful of employees that should ever send a SSN other than their own - this may not be a part of your business or it may be a huge part of your business so you need to make sure you understand it and correctly monitor for it.

From a people standpoint, each and every person who has access to your systems should be educated and equipped to be a part of your security force. This includes employees, clients, vendors, and anyone else with an ID. Each active ID should be considered a door you need to put a lock on. Ultimately, you cannot control the human factor, so proper identity management and role-based access is critical and must be coupled with monitoring/auditing to be effective.

Communication is another vital component to your defense strategy. It seems obvious, but most organizations don't have a communication plan in place before the first time it is needed. At the highest level, you need communication before, during, and after an attack scenario. This naturally expands itself when you consider your lines of business – IT will have one set of communication plans which will largely comprise of an incident resolution, while Marketing, PR, Finance, HR, and Vendor relations will require uniquely different approaches.

## **Conclusion**

Cybersecurity crime and the defense against it will be pervasive in our lives for the foreseeable future and if you fail to take meaningful action, you can almost guarantee your shareholders that something bad is going to happen. On a relative scale, damage to reputation, data loss, financial loss, and business solvency are likely consequences of inaction or improper action.

The war is mounting, and the bad guys have the advantage. Humans write the code that protects our systems and data and because of that, mistakes will inherently be made. There has never been an easier or less risky time to take to Cybercrime as a profession if you are wired that way. Not to sound cliché, but now is the time to begin taking Cybersecurity seriously and

to transform the mindset and practices of your organization. Look no further than the staggering recent growth of the Cybercrime Insurance industry as proof in the pudding (a Google search of “Cyber Crime Insurance” yielded over 8.6 million results in less than .3 of a second!)

The comforting news is that there are measures your organization can take to better defend and protect against the multitude of channels in to and out of your organization. Developing a strategy and committing to defense today can amply protect assets and what the future holds for your organizations’ success.

Trexin Consulting experts have walked in your shoes and developed successful strategies that can be executed immediately. Staying at the forefront of Cybercrime from both “good guy” and “bad guy” perspectives is the edge you need to ease this new burden of doing business in the electronic age.

We can help, call us today.



This TIP was written by Ralph Carlone, who specializes in cybersecurity, program and project management, business process management and systems management. Ralph welcomes comments and discussion on this topic and can be reached at [ralph.carlone@trexin.com](mailto:ralph.carlone@trexin.com)

---