WHITE PAPER

Modern Defense in Depth

SYSTEMS engineering

WHITE PAPER

Modern Defense in Depth

A few short years ago, business information networks were largely protected from outside attacks through a 'moat and castle' strategy that typically included a strong firewall and antivirus software. This unified, single-line-of-defense strategy generally allowed business-as-usual operations to safely take place within the confines of the organization's four walls.

Trouble is, that's not where business happens anymore.

SIMPLY BUILDING 'BIGGER WALLS' IS NO LONGER AN EFFECTIVE SECURITY STRATEGY.

The new reality of cybercrime activity necessitates a shift from the traditional 'moat-and-castle' data security approach to an evolved, more modern defense in depth strategy to protect our digital estates and force would-be attackers to navigate a series of multiple, disparate checkpoints before gaining access to the trove of data (and financial booty) they seek to plunder.

In this white paper, we identify the tactics businesses can use to properly defend their data—wherever it may be.

SYSTEMS engineering

WHITE PAPER

Modern Defense in Depth

WHAT'S AT RISK? EVERYTHING.

According to the 2017 Cybercrime Report by Herjavec Group, cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This startling increase reflects a significant loss in economic productivity. Money that could be reinvested in the business or distributed to shareholders must now be used to pay ransom, regulatory fines, and data breach clean-up expenses.

The potential impact can completely ruin the business—for those who are unprepared can find themselves unable to rebound either financially or otherwise after its reputation is ruined from the effects of the attack.

Ponemon 2018 Cost of a Data Breach Study

$3.86M
average cost of a data breach.

27.9%
likelihood of a reoccuring material breach over the next two years.

$148
average cost per lost or stolen record.

6.4%
average total one-year cost increase.

4.8%
one-year increase in per capita cost.

27.9%
average cost savings with an Incident Response Team.

DOING BUSINESS ANYWHERE = POTENTIAL THREATS EVERYWHERE.

The rise of cloud-based services, employee mobile device usage, and the role of social media in our lives has created an ad-hoc business network environment where information is constantly being saved, sent, received, and accessed from dozens, if not hundreds, of locations around the world.

At the same time, cybercriminals are becoming increasingly sophisticated, often collaborating to identify potential weaknesses, mimic legitimate electronic communications such as email, and develop malicious software applications. Once they gain access to a working credential, they move incredibly quick to get what they want.

Their predatory ways are paying off and hurting the bottom line for many businesses. Cybercriminals have created significant data security challenges for all businesses but especially for smaller and medium-sized businesses that find themselves in the cybercriminal's cross hairs.

The truth is that all too often businesses lack the resources or available finances to implement effective security defenses on their own, making them an easy target of opportunity.

Sadly, most business owners know they are not safe, yet they feel powerless to improve their posture on their own. In fact, a Ponemon Institute research report found that only 21 percent of small and medium-sized businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.

A BALANCING ACT. SECURING SHARED ACCESS.

Gone are the days when a network firewall and antivirus software are enough to thwart a malicious attack. As previously mentioned, increased mobile device use and the proliferation of cloud-based business services—*i.e. Dropbox, Google Docs*—have made networks more distributed and prime targets for hackers if your defenses have not evolved to care for the data in and around the digital estate.

In the past, network administrators could rely on limited access and limited connections, tightly controlled at the perimeter, without verifying a user's identity each and every time, but the reality of today's on-demand service world dictates that connections between users and business applications will be sporadic, distant, and time sensitive which means verifying users' identity has become foundational to any business' security strategy.

While the basic need for a layered approach to security has not changed, exactly how and where your network security solutions are deployed has.

Since a greater amount of day-to-day work is now being done through mobile devices and from cloud-based applications, the number of potential places where your network is vulnerable for an attack is now equal to the sum of every network-capable device owned or used by your employees.

Attacks, whether accidental or intentional, can give the appearance of originating from inside the network itself. A data breach does not always require a criminal working to infiltrate from the outside. Sometimes, sending an unsecured spreadsheet of sensitive information through a web-based email account can be just as dangerous.

That's why passive approaches to security, such as legacy antivirus and firewalls are no longer enough to accurately and efficiently spot and stop sophisticated attacks from well-trained and well-equipped cybercriminals.

THE CHALLENGE: VERIFY ON-THE-FLY.

IT professionals are now tasked with having to develop and deploy network security systems that can instantaneously identify, verify, and deliver information that is constantly in motion, allowing legitimate business transactions to occur without delay.

All this in a world where individual identities are hard to verify, and intruders are hard to see until it is too late.

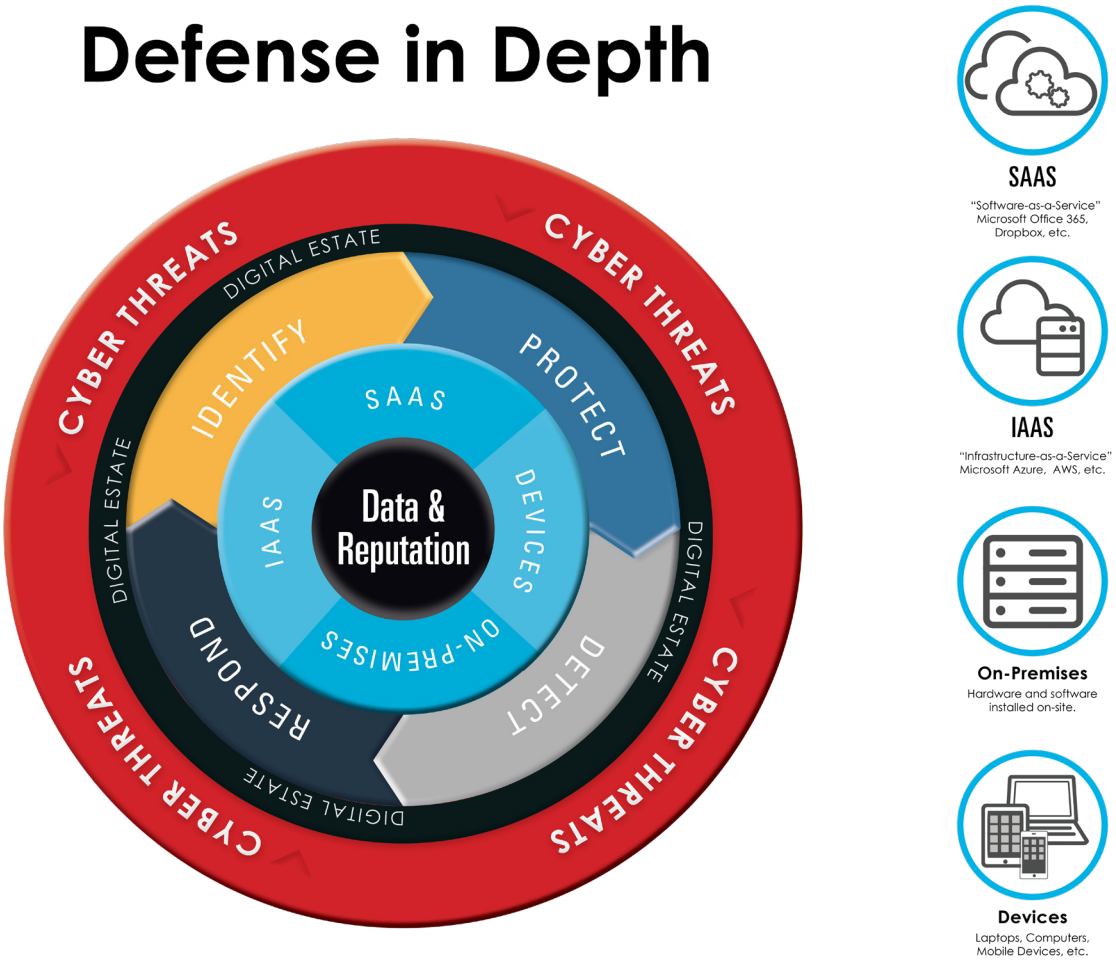
SO, WHAT'S A BUSINESS TO DO?

Over the last few years, Systems Engineering's security team has advised many of its clients to take steps to make their networks less attractive to cybercriminals by implementing a modern defense in depth approach to security.

Whereas previous security methodologies relied heavily on the strength of a single, continuous wall to repel all suspicious activity (outside of the network), the strength of the modern defense in depth approach is found in its strategy. More specifically, businesses must understand the breadth of their digital estates and apply the right security controls to each segment in the estate.

EMPLOY A MODERN DEFENSE IN DEPTH APPROACH.

Fortunately, shifting to a modern defense in depth approach for security does not require businesses to completely abandon all the systems they already have in place. Rather, today's defense in depth approach represents a cumulative approach to network security where the addition of each new control increases the effectiveness of the entire system, guarding against a multitude of attack methods.



While the right security controls added to an existing environment will improve its effectiveness against a cyberattack, this does not mean businesses should hastily begin adding on the latest, trendiest security tools. If there is one thing we have learned over the past several years, it's that more is not always better. Instead, as you add additional depth to your security posture, understand the role that old and new solutions play and how they integrate with and complement each other.

An evolved defense in depth security protocol can include many different elements and should adapt as new threats emerge.

Today, we consider the following to be your target set of measures to keep your organization secure:

- **Written information security policies**
- **Security awareness training and testing for employees**
- **Effective backups and a Disaster Recovery (DR) plan**
- **Multi-factor authentication (MFA)**
- **Device monitoring and patching**
- **Encryption of data at rest**
- **Email encryption**
- **Endpoint security**
- **Periodic Security Assessments**
- **Security Operations Center**

2018 VERIZON DATA BREACH INVESTIGATIONS REPORT

Fast Facts

73%
of cyberattacks were perpetrated by outsiders.

58%
of victims were small businesses.

68%
of breaches took months or longer to discover.

ACHIEVING A MODERN DEFENSE IN DEPTH APPROACH.

Acquiring security tools and implementing them without a strategy won't necessarily help businesses to achieve their security goals or meet their regulatory obligations. Security is a process and there are critical steps businesses can and should take in order to achieve an effective modern defense in depth approach.

STEP 1: BEGIN WITH DEFINING YOUR SECURITY POLICIES.

Developing an overall corporate vision and operational guidelines in the form of an information security protocol guidebook provides key personnel with the opportunity to document, then clearly articulate, how an organization (and the people within it) will interact with company information.

An effective security policy should include the following components:

- **A statement describing how and why the organization protects sensitive information. Include any standard practices, such as what constitutes appropriate/effective personal passwords that are in use within the organization.**
- **An acceptable use policy for all employees to understand exactly how they are expected to use and secure company-owned equipment. A policy statement that describes the appropriate use of personal (bring your own device or BYOD) technology devices to access company data, including the organization's right to completely wipe a device should it become lost or stolen.**
- **A social media policy that sets clear expectations about the way(s) in which an employee represents the organization with their personal use of social media.**
- **Documentation that describes the activities that take place during the annual employee security awareness training event(s) as well as the ongoing occurrence of periodic, simulated email phishing attacks instituted by the IT department.**

STEP 2: KNOW WHO WANTS TO ACCESS TO YOUR VALUABLE DATA.

Today, your applications and files are no longer all contained within your four walls and you need to know who is knocking at the door before you let them in. While this risk is not new, verifying a users' identity and what they can have access to has become critical as businesses are now more exposed to a mix of on-premises and cloud-based applications.

Most businesses choose to start with a centrally managed identity for all their employees—a Windows domain user name and password, for example. While some businesses have made it mandatory and require complex passwords, a substantial number of businesses still do not. This is due to the perceived inconvenience of creating and remembering numerous and varying complex passwords. And even fewer have implemented multi-factor authentication (MFA) for similar reasons in addition to the costs.

Because most data breaches begin with the compromised credentials of a legitimate network user, creating a system of identity verification that uses an MFA process can greatly reduce the chances of a cybercriminal successfully gaining access to a secure network by posing as an authentic user.

Multi-factor is the concept of getting extended proof a user is who they say they are by having them provide something they KNOW, something they HAVE, and something they ARE. For example, you might first provide a password, followed by entering a unique key that proves you have control of your physical device. This would provide two factors of authentication—something you KNOW and something you HAVE. You may also choose to add fingerprint or facial recognition as a third factor of authentication which would be something you ARE.

STEP 3: EMPOWER YOUR USERS WITH TOOLS TO HELP THEM BE MORE SECURE.

The most engaged employees feel safe and trusted at work and these values must be considered as you work to implement security improvements.

There are some easy ways to become more secure and make the workplace securer while encouraging productivity:

- **Mentioned previously, give your staff access to the latest security training and, if you're able, go the extra mile by conducting lunch and learns with industry experts. This additional education reinforces a culture of security and provides common values for staff to work with.**
- **Implement email protection tools that filter dangerous email, protect against dangerous links, and provide visual warnings to users. This will help take the pressure off staff and make it easier to do the right thing.**
- **Have systems patched and monitored to shore up vulnerabilities and stop attacks in their tracks. This way, even if a user makes a mistake, you have time to remediate it before any damage is done.**
- **Watch your network for malicious traffic by having a platform and a trained team of security experts to look for anomalies. Experts can investigate any unusual events, protectively block any suspicious packets, and review dashboards to catch stealthy cybercriminals who are clever enough to make it through your series of protections.**

STEP 4: HAVE A PLAN FOR REMEDIATION AND RECOVERY.

To be able to successfully recover your business from the impact of a cyberattack and/or breach starts with acknowledging and planning for the eventuality of one actually occurring.

The remediation planning process starts with bringing together stakeholders throughout your organization to brainstorm the threats and vulnerabilities your organization might be exposed to (i.e. ransomware, DDOS, virus, etc...), assessing the impact each attack could have on the business, and defining remediation plans to get business operations back up and running.

Remediation planning should involve developing the following items:

- **Create a written Disaster Recovery Plan and test its effectiveness annually. Testing could be as basic as a table-top exercise to ensure your plan works as designed.**
- **Establish a written Incident Response Plan that addresses the specific actions during a potential data breach.**
- **Implement a system to collect and manage audit logs, traffic history, and other forensic network data to help identify valuable information about the attack. Yes, physically monitoring and capturing information stored in these logs is just as important even though much of the activity now happens outside your physical network.**
- **Consider purchasing cyber insurance. Some policies will include services to help companies manage the remediation process.**

By clearly defining remediation timelines, goals, personnel roles, and responsibilities, businesses can identify where technology or human-power weaknesses exist and take the appropriate actions to address them.

THE ROAD AHEAD.

There's little doubt that threats from cybercrime will only increase over the next several years. The payoffs are simply too great for criminals to ignore.

As we look ahead, the trend towards more cloud-based, adaptive learning security solutions will continue to make strides against the relentless pace of cybercrime attacks worldwide.

These solutions, comprising a modern defense in depth security strategy, represent the best protection against the shape-shifting capabilities of cybercriminals and cyberterrorists intent on disrupting our online world for their own financial gains.

In the same way that advances in the tools and technologies used in medicine, transportation, and manufacturing have kept each industry moving forward, the time has come for new, more agile, more intelligent security tools to emerge as a much-needed line of defense between good and evil.

ABOUT SYSTEMS ENGINEERING

Systems Engineering is an IT strategy and managed services provider delivering world-class technical and business solutions to enable the exceptional within organizations. Established in 1988, Systems Engineering is a 100% employee-owned serving more than 500 legal, healthcare, financial services, and government clients nationwide. Headquartered in Portland, ME with an additional office location in Manchester, NH, the company has a team of 150+ who are available 24×7, 365 days per year to serve the needs of its clients. Known as a forward-thinking, modern technology partner, Systems Engineering seeks to enhance business by providing superior managed IT, security, cloud, and consulting and IT leadership that allows companies to grow and prosper.

To enable the exceptional within your organization, visit systemsengineering.com or call 888.624.6737.