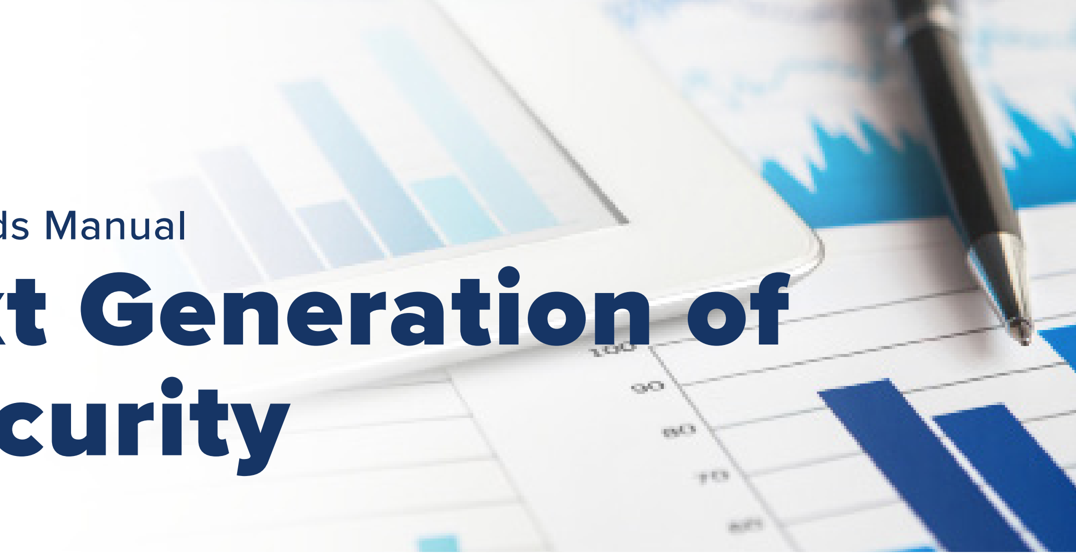


Management Methods Manual

The Next Generation of Data Security

INTRODUCTION

With an industry as established as construction, the concept of data security is a relatively recent concern. Buildings are still built and maintained with physical tools and manpower, but the planning and operations process have shifted away from paper to computers, tablets and cell phones. The amount of data being generated on each project is accelerating, as is the importance in protecting this data.

Between 2020 and 2021 almost 1 in 6 construction companies reported a ransomware attack. This is a fraction of the actual total since many organizations do not disclose breaches. By 2025 the world is expected to have more than 50 billion connected devices and computers. At the current infection rate trends this means that at any given time, there will be roughly 5 billion infected or weaponized devices and computers online.

Securing our operations, client, financial and personnel information from these serious and persistent threats should be a top priority in your company. Roughly 60% of all small to midsized corporations are unable to survive once they are hit with a massive Cyberattack like ransomware. Many more corporations will be disrupted as their customers also experience cyber attacks which may result in work stoppages and lost revenue for the company. Anything related to technology or cyber security can no longer be taken on faith. It should be protected like any other company asset, but with different tools and strategies. This article is intended to provide guidance and insight of current tools and techniques to protect your data and operations.

Cyberdefense strategies are the rare occasion when enforcing an "all or none" policy is the only way to truly mitigate all threats on the planet. A network that is 90% defended is a network with a 10% gap that hackers can drive a virtual truck through. To begin, it must first be understood the concepts that govern Cybersecurity and government compliance as a whole.

TIP

Construction is still a hands on process but the planning and operations have moved to computers.

THE C.I.A. STANDARD FOR DATA SECURITY

TIP

There are 3 major security issues that need to be addressed to properly defend your data.

When dealing with Data Security, the standard security dimensions that should govern your cybersecurity strategy must be understood. Based on the main government compliance standard[1], there are three major security dimensions we must address when properly defending data; Confidentiality, Integrity, and Availability. This is known as C.I.A.

- **Confidentiality** is the process by which we ensure that the data stored for clients and customers is protected. This includes encrypting data to proper standards, defensive hardware and software such as firewalls and antivirus software that wraps the data to prevent hacking and other malfeasance, and ensuring that the method for storing the data is protected from threat.
- **Integrity** is the methodology that ensures only authorized personnel can access the data as well as ensuring that a tiered method for levels of access is adhered to so no unauthorized personnel can access, copy or change the data.
- **Availability** ensures that proper backups and redundancies are in place so the data has optimal uptime as well as the ability to restore quickly in case of a threat, whether it's a natural disaster or hacking event.

For all of C.I.A., monitoring and reporting is critical to ensure that no compromises have occurred. Network configuration must then be considered in order to properly defend data adhering to the C.I.A. standard.

THE ZERO TRUST NETWORK CONFIGURATION MODEL[2]

IMPORTANT

ZTN - Zero Trust Network

To configure a network with C.I.A. protection in mind, an approach that utilizes isolation and verification is necessary. The Zero Trust Network (ZTN) configuration relies on segmenting (isolating) computers, servers and all other networked devices. This creates a network where each device of any kind is siloed, filtered by threat management and only allowed to communicate with authorized devices after verifying that it's free from threat. The segmentation is important as it protects the rest of your network is protected if one computer is compromised.

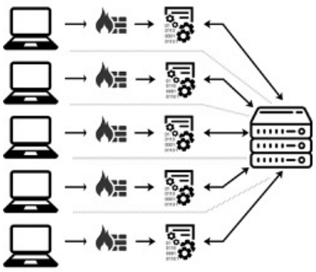
A properly built ZTN will not impede the user in any way, including performance, unless a threat is detected. When a threat is detected the device/computer is automatically shutdown and fully isolated from the network to ensure that no viral infections can outbreak and infect others.

[1] Set forth by the Federal Information Security Management Act (FISMSA)

[2] Conceived of by Forrester Research, the Zero Trust model has been widely adopted for advanced Cyberdefense implementations ranging from Small Business to Enterprise

Zero Trust Network Example:

5 desktop computers use a single server in a network. The server holds the data and all 5 computers require access to the server. In a Zero Trust model, the following configuration would be implemented:



- None of the 5 desktop computers would be allowed to talk to each other over the network, eliminating the chance of one laptop infecting another.
- The 5 desktop computers accessing the server would first have to pass through a threat management system, such as a Next Generation Firewall (NGFW) and verify that they are free from infections before being allowed to access the data. This ensures that no computer can infect the server and vice versa.
- The server's data would be segmented to allow visibility and access based on the computer or user's need. This ensures that even if an infection does bypass the defenses the possibility of total outbreak infection is relegated to a select group of data.

Currently, over 99% of all networks in the world rely on a Perimeter only defensive strategy and not the Zero Trust model. This means that the network has a firewall of any level sitting between the Internet and the internal computers/servers/devices on the network. Any computer/server/device "behind" the perimeter that the firewall creates is allowed to communicate with every other computer/server/device. Thus, if a pervasive infection hits one device it can possibly infect all the others because there are no internal controls checking the internal communication for threat.

SECURING THE PERIMETER: THE NEXT GENERATION FIREWALL

The foundation of all Cyberdefense strategies begins at the infrastructure level, starting with the perimeter of the network. As defined above, the perimeter is what a firewall creates to protect the network against the largest threat vector: the Internet. Not all firewalls are built the same and with several changes to USA data security compliance laws the requirements for a firewall that will properly defend a network have increased. Whether your business falls under compliance or not, a next generation firewall is a requirement

! IMPORTANT

The perimeter is what the firewall creates to protect the network.

for defending your network correctly. Anything less and there is a massive vulnerability in your Cyberdefense strategy.

Your network should be employing a firewall that has the following features:

- **Unified Threat Management (UTM).** This is a term that encompasses the firewall's ability to run Antivirus in order to check all traffic for threat, vulnerability defense, intrusion prevention systems and a way to easily view all threats through the interface.

- **Zero Day Updating.** This is the firewall's ability to have its defenses updated against new threats less than 24 hours after the initial discovery or outbreak of the threat anywhere in the world.

- **Sandboxing.** This is the firewall's ability to analyze unusual traffic that isn't flagged immediately as a threat, stop the traffic from entering or exiting the network and sending it to a sandboxing service, whether the sandbox is onsite or in the cloud, for analysis.

- **VPN with Multifactor Authentication.** Coverage for mobile devices and computers through a Virtual Private Network (VPN). This will ensure that even when the device is outside of the network all Internet traffic is routing through the firewall to ensure it has the same level of defense as the internal computers. Since mobile infections are the largest growing threat vector, this point is just as critical as the others.

- **Real-time Monitoring.** This allows authorized Cybersecurity personnel to be alerted to threats immediately and begin the remediation process to ensure that no possible threats are successful.

- **Integration for Identity Management.** This helps to ensure that the behavior of the users is being checked to ensure that they are logging from known locations and not hijacked by attackers. This also helps to integrate Multifactor Authentication, Biometric Authentication and more into the network.

Firewall Recommendation

- Palo Alto Networks (PA). More Fortune 100 and Global 2000 corporations use PA than any other firewall brand and for good reason. PA's outbreak threat detection is by far the fastest detection and inoculation time globally and they are the leader in new virus discovery. They have products geared towards small and medium and while they're slightly more expensive than the average NGFW their detection is unparalleled and worth the extra cost.

- No other recommendation for firewalls. The firewall is the most critical piece of a Cyberdefense strategy in terms of hardware/software, to install anything less than the best can compromise the entire design.

NETWORK SEGMENTATION

Critical to any Zero Trust configuration is segmentation. Segmentation is the isolating of computers and devices so that they cannot interact with anything else on the network except for those computers or devices they require access too. This configuration is achieved at the hardware level with a combination of Next Generation Firewalls and Network Switches. There are varying levels of segmentation that can help your organization achieve a higher level of security through isolation.

The most common forms of network segmentation are:

- **Individual segmentation.** This is a design that requires all devices and computers to be completely separated from all other devices except those devices and computers they are authorized they have access to. This mitigates an outbreak infection to only the computer or device infected thus ensure no infections can go beyond the initial computer. This is considered the optimal Zero Trust configuration. As an example, if all corporate data resources are in the cloud there is no reason for any computer or device to talk to each other thus it is optimal to not have them to do so. The chance of an outbreak infection is nil.

- **Group Segmentation.** This is a design that allows computers in a specific group to access each other, even if there is no need for them to have access to each other, however the group cannot access other groups on the networks. This mitigates an outbreak infection to the group only.

IMPORTANT

Segmentation is the isolation of computers & devices so they cannot interact with anything else on the network except other devices it requires access to.

For example, if your company has an Accounting Department and a Sales Department an outbreak in the Accounting Department may infect every computer in Accounting but the Sales Department will not be affected. This option is chosen primarily as a cost mitigation factor since less threat detection routing is needed.

- **Mobile Segmentation.** This is a design that isolates any mobile devices or computers from the main network or isolates one physical location from another. In this method an outbreak on a mobile device or computer cannot infect the main network. Also, one physical location will not infect another. As an example, if your company has a main office and a production facility, the main office will not infect the production facility.

Recommended Equipment

Firewalls:

- Palo Alto Networks. See "Securing the Perimeter" section for explanation.

Networks Switches:

- Brocade. Enterprise switches at a more reasonable price, Brocade runs the balance between excellent performance, features, longevity and price.
- Secondary Recommendation: Arista. Considered the best switch on the market today, Arista has the best features and performance of any switch on the market. Comcast's entire new fiber infrastructure is on Arista. The only downside is the price, which is why Brocade is ideal for small to midsize businesses.

LAYERING INTERNAL SECURITY: ENDPOINT DETECTION RESPONSE (EDR) SOFTWARE & DNS FILTERS

While the primary defense for infections and filtering is at the perimeter of the network with a Next Generation Firewall it is important to have backup scanners and filters to fill in any gaps that the firewall cannot defend against. An employee who picks up a flash drive from the local coffee shop could be

IMPORTANT

It is important to have backup scanners and filters for any gaps that the firewall cannot defend against.

walking an infection past the infrastructure defenses and plugging it straight into a computer for example. A mobile laptop that loses it's VPN connection has to route the internet on its own also needs to make sure it can properly filter the internet for threats and defend against viruses.

It should be noted that no EDR is perfect at detecting and remediating threats. This is one of the reasons why the Next Generation Firewall is so critical to the defense strategy as most of the traffic going to the computer will go through the firewall most.

Not all EDR solutions or DNS Filters are equal. Ensure that your solutions have the following:

Anitvirus:

- Support for Centralization of reporting and alerting
- Realtime inoculation
- Realtime remediation of Zero Day threats
- Deep or Machine Learning artificial intelligence to understand the behavior of an infection and how it could spread in the network
- "Next Generation" antivirus features such as kernel metadata analyzation and behavior pattern recognition

DNS Filter:

- Cloud based DNS routing
- Policies and control procedures for Whitelisting and Blacklisting websites
- Advanced reporting and analytics for a complete overview of online website threats to users.

TIP

Imagine you, the contractor, are a car salesman. You should make sure they buyer (the owner) can pay for the car before you agree to the sale.

Recommendations

Antivirus Software[3]:

- Deep Instinct (DI). All virus scanners are vulnerable. DI is less vulnerable. They currently have the best threat detection system of all software-based antivirus software on the market and are competitively priced.
- Secondary recommendation: Crowdstrike Falcon. Not as effective as Deep Instinct however it is both capable of detection and it considered both a major player in EDR and also competition to Deep Instinct.

[3] EDR rankings by testing change constantly. A review of possible EDR solutions should be performed before purchase to ensure the best possible option at the time.

DNS Filter[4]:

- Cisco Umbrella (formerly OpenDNS). The best and largest DNS Filter on the market by far and rather inexpensive. In terms of software-based DNS Filters, Umbrella is not the only choice but it's the most effective to date.

BLOCKING INBOUND EMAIL THREATS: SPAM FILTERS

TIP

Since email is the most widely used way to communicate, a spam filter is very important.

As email continues to be a primary form of communication, a spam filter is required. There are two primary types of spam filters: cloud based or on-premises.

In all cases a cloud spam filter is preferred for multiple reasons including:

- The ability for the spam filter to inoculate itself in real time much faster than an on-premises spam filter appliance can.

- Denial of Service email attacks will not affect your local network since the cloud spam filter provider will take the attack instead of your local Internet connection.

- The cloud optimizes the performance of your office's Internet connection by forcing all incoming emails to be filtered offsite first. With

Cloud Based Spam Filter Recommendations:

- Proofpoint. Considered the industry leader in spam threat detection, Proofpoint is used by more Fortune 100 and Global 2000 corporations, like the Palo Alto Networks firewalls, and is priced for small business.
- Avanan. Newer than many of its competitors, Avanan's threat detection model has been heralded as possible next generation approach to spam filtering.

[4] A DNS Filter can be enabled in a Next Generation Firewall, which also offers an excellent solution. However, for mobile devices a VPN will be required to use it. Palo Alto Networks is the best hardware-based DNS Filter on the market.

DEFENSE FOR MOBILE DEVICES: NO LONGER AN OPTION

The largest threat vector on the planet, currently, is mobile phones. More infections for Google's Android and Apple's iPhone/iPad are released than any other operating system including Microsoft Windows. There is a mindset that mobile devices are safer which is a myth. They need defending and in a Zero Trust Network configuration, mobile device defense is a critical piece of the design. Laptops and other mobile computers must adhere to the same data policies as the computers within the office's network.

TIP

Mobile device defense is a critial piece of design in a Zero Trust Network.

The optimal mobile device configuration is as follows:

- **Antivirus or EDR software.** See above section "Layering the Internal Security" for explanation.
- **DNS Filter.** See above section "Layering the Internal Security" for explanation.
- **Virtual Private Network (VPN).** A VPN ensure that all mobile Internet traffic will route through your Next Generation Firewall thus ensuring an extra layer of security, encryption and privacy.
- **Encryption.** All devices on all platforms should be fully encrypted using AES256 encryption. This ensures integrity and confidentially if the device is lost or stolen.
- **Mobile Device Management (MDM).** This allows total control of the mobile device. From GPS tracking, remote wipe and visibility to patching and backups, having an MDM is essentially a requirement to ensure data security.

Note: A "Bring Your Own Device" (BYOD) policy within an organization is never recommended. Various states have data privacy laws for the users, which means that things like remote wiping corporate off of a personal phone could constitute the basis for legal action against the corporation. Further, ensuring all security policies are adhered to on a personal phone cannot be fully enforced, usually due to privacy laws.

Android & Apple Recommendations:

- **Antivirus or EDR.** Deep Instinct is consistently rated among the top Android antivirus apps and has held the number one spot for several months.
- **DNS Filter.** CleanBrowsing's app is top rated though this category should be deferred to an always-on 24/7 corporate VPN. Therefore, this app acts as a backup or is used in a scenario where a VPN is not available.
- **VPN (non corporate firewall related).** VyprVPN is inexpensive, allows multiple devices on a single account and has a worldwide network of encrypted servers to connect to.
- **VPN (corporate firewall related).** GlobalProtect by Palo Alto Networks. If you have a multi-location network with Palo Alto your mobile devices, thanks to GPS, will automatically connect to the closest office and give the mobile device the full protection of the enterprise firewall which defends the corporate offices.
- **Encryption.** The integrated encryption native to Android runs military grade AES encryption and should be enabled with a password between 8 to 14 characters long and should include all four character sets (Uppercase and Lowercase letters, numbers, special characters such as ?, &, and $)

Mobile Device Management Systems Recommendations:

- AirWatch by VMWare is currently the industry leader with a robust set of mobile management tools and is highly scalable for a growing workforce.
- Secondary recommendation. MaaS360 With Watson by IBM is another industry leader with an excellent reputation though lacks the flexibility of AirWatch

MAINTAINING AVAILABILITY: BACKUPS, BACKUPS, BACKUPS

In terms of Data Security, backups are one of the most important aspects of a good Cyberdefense strategy. The unforeseen can happen and even the best defense has the possibility of being innovated around by an experienced hacker. On top of this, surviving natural disasters, or acts of God, is of paramount importance to a corporation. Ensure maximum uptime as fast as possible ensures the survivability of the company.

IMPORTANT

Always backup your information. If something happens and you have to shut down, having a backup ready to go will make recovering easier.

Today, an important part of the backup design now includes the cloud. In a 2017 survey performed by the Cloud Security Alliance for the first time in history more corporations are trusting the cloud for data security than their own onsite equipment. This is for various reasons including the uptime capabilities, the cloud ability to patch and update against threat faster than the company and also advanced monitoring for threats and integrity.

When designing a back strategy, the following elements should be included:

- Onsite backup for fast restore in case of deletion, infection or corruption.
- Cloud backup that is a duplicate of the onsite backup to protect the organization from loss of onsite infrastructure or infection of onsite backups (which is a growing threat vector).
- Image based backups for both onsite and cloud backups allow for fast restoration of a failed physical or virtual environment.
- Virtualization of backup images both onsite and in the cloud. If a physical server fails a duplicate of the server should be able to come online quickly either onsite or in the cloud to minimize disruption.
- Immutable storage on-premises to help thwart attacks against the backup infrastructure by ensuring that backups cannot be altered once they're finished backing up.
- Real time incremental backups or snapshots. This can be adjusted to the needs of the corporation in terms of data availability and compliance laws for revision history. Companies should be backing up no less than 12 times daily and many do it with much more frequency than this depending on cost to business versus cost of downtime.
- Encryption. All backups should be encrypted using AES256 encryption in case of loss or theft of the backup files.

Backup Software Recommendations:

Windows:

- Storagecraft ShadowProtect is currently the small to medium business industry standard for Windows infrastructure as it allows for imaging of systems incrementally, can be moved to the cloud easily since many Cloud providers use Storagecraft technology.
- Secondary Recommendation. Veeam is another solid player targeting small to midsize business.

Virtual/Linux:

- Veeam is an industry leader for backup technology and disaster recovery. Many consider them the gold standard to the balance of price versus performance.
- Secondary Recommendation. Commvault is another industry and would take the top spot here if it wasn't for cost.

Cloud Providers (Small - Midsize Business):

- Datto. A major player in cloud backup, they have expanded rapidly over the last few years yet still have a focus on delivering excellent customer service.
- Secondary Recommendation. Axcient is the top rival to Datto in the small to mid-market. Both choices are excellent through most find Datto easier to work with.

KEEPING UP WITH THE HACKERS: REMOTE MANAGED MONITORING (RMM) FOR PATCHING, UPDATING AND POLICY ENFORCEMENT

No one is a fan of patching and updating. It takes time and keeps the users from doing his or her job. However, patching and updating is beyond critical. Software and hardware vendors patch their offerings for two primary reasons. First, they patch for performance. Second, and more importantly, they patch for security. Most patches released are to fix vulnerabilities and if these are being skipped then the network's defenses are seriously compromised.

It's beyond important for a company that patching and updating is removed as a choice for the employees. Several studies have shown that users, and we've all done this, will continuously skip patching and updating and the

TIP

Always take the time to patch and update! This is an easy way to keep your security running as well as possible.

longer it's delayed the larger the vulnerability becomes. It is for this reason that a good patching policing consists of the following:

- Centralized Patch Management so IT personnel can view all device patch levels in real time and remediate faster.

- Scheduled patch times that the whole organization acknowledges, and IT enforces. This way patching can be done easily and usually after hours.

- A vetting process for patches. Sometimes new updates can crash devices or wreak other kinds of havoc on a network. IT personnel that are able to test patches in the environment without user disruption helps ensure no outages due to updating.

- Periodic review of patching to ensure all devices are up to date but also to identify any users that are consistently behind and remediate the behavior. Patching should be a considered part of the job.

Mobile Device Management Systems Recommendations:

- AirWatch by VMWare is currently the industry leader with a robust set of mobile management tools and is highly scalable for a growing workforce.
- Secondary recommendation. MaaS360 With Watson by IBM is another industry leader with an excellent reputation though lacks the flexibility of AirWatch

The above RMM recommendations also include the ability to enforce policies on the computers above and beyond the standard policy enforcement. Centralized control of user access, encryption policies, installation of third-party software policies and more are critical to ensuring that users don't accidentally remove key defenses from the computer or accidentally install an infected program.

MONITORING FOR THREATS AND VULNERABILITY: REAL TIME REMEDIATION

Above and beyond patching and updating is monitoring for threats. Organizations are under attack 24 hours a day and overwhelmingly most do not realize this. External facing firewalls are always being scanned and tested for vulnerability by hackers. This is an automated process for them so they will hit hundreds to thousands of firewalls a day looking for anything they can exploit. If they find one, then they will actually go to work on breaking in. A good monitoring system paired with excellent defensive firewalls go a long way to ensuring that these attacks are identified and stopped before damage is done.

IMPORTANT

Patching and updating is good but moitoring threats is the cherry on top. Hackers never sleep.

There are many types of monitoring solutions but one of the core options businesses choose is a Security Information and Event Management (SIEM) solution.

Outside of the computers, the following infrastructure should be monitored in real time for threats:

- Firewalls, as are the first line of the defense and most likely to come under attack regularly.
- Wireless Access Points, since they can be hijacked and attacked since they broadcast an entry point into the network
- Network Switches, especially L3 type switches, can be hijacked and used to perform a “Man-in-the-Middle” data capture attack.
- Network Printers can be hijacked to either print out negative materials, hijacked to be used as a bandwidth weapon against the network or other targets, or data printed can be captured and read by hackers.
- IoT devices such as video cameras, DVRs and others can be hijacked and weaponized against targets.

A good monitoring solution will monitor these threats in real time, act to stop the attack and also backup firmware configurations for quick restore in case a hacker is able to hijack a device and reconfigure it.

Real-time Monitoring & Remediation Recommendations:

- Security Fanatics' Blokworx Monitoring is the balance between cost and performance. Vendor agnostic, they support virtually all hardware that can be monitored with excellent remediation services.
- Secondary Recommendation. IBM Resilient is the best service on the planet with no real competitors. They also have an IBM Watson AI detection system that is unrivaled integrated into Resilient. They're a secondary recommendation only because most businesses find the cost of their service to be "outrageous."

STOPPING THE EXTORTION ATTEMPTS: DIGITAL RIGHTS MANAGEMENT (DRM) & DATA LOSS PREVENTION (DLP)

One of the biggest concerns with cyber-attacks to emerge in the last few years is the theft of company data and its extortion. Many companies experience this exact scenario: their data has been encrypted in their office or in the cloud thanks to ransomware but then they also receive a ransom note stating that the attackers will release or sell their data in the Dark Web, which can have severe consequences to the financial health and reputation of the business. Fortunately, a DRM/DLP solution helps protect organizations against extortion of this nature.

! IMPORTANT

Too many times a hacker will take a company's info and hold it for ransom until they are paid. Don't let that happen to you.

A good DRM/DLP solution will have the following characteristics:

- Integration with Identity Management solutions to help verify that users are accessing data are legitimate.
- Encryption of files and folders that is agnostics to where the data is stored.
- A key management system that is separated from the infrastructure where the data is so no attacker can capture the keys that unlock the data by hitting a single system.
- Alerting when files are attempting to be access but failing to authenticate.

Real-time Monitoring & Remediation Recommendations:

- SecureCircle. They run the balance between cost and effectiveness and use strong encryption for security as well as cloud based hardened key management.
- **Secondary recommendation:** Code42. A solid enterprise choices for DRM/DLP however they are much more expensive than SecureCircle.

IDENTITY MANAGEMENT: UNDERSTANDING REAL USERS FROM MALICIOUS ATTACKERS

With billions of usernames and passwords in the Dark Web, with millions more being added daily, one of the most critical aspects of defense is to protect the identities of the users, systems and applications as they access and interact with organizational data. Identity Management solutions understand the behavior of the user thanks to artificial intelligence and have the ability to block a user from gaining access to any aspect of the network when a threat is detected.

TIP

Identity Management solutions can understand a user's behavior thanks to AI. This helps it notice when someone else is trying to get in.

A good Identity Management solution has the following characteristics:

- Single Sign-on (SSO) capabilities to bring all accessible assets in an organization into a secure portal that can be monitored and defended.
- Adaptive Multifactor Authentication to ensure that no single username and password can compromise the SSO or any asset of the organization.
- Behavioral threat identification that includes, but is not limited to, an understanding of normal user login routines, geo-fencing of users, geo-velocity of logins, biometric identification and more.
- Real time alerting and blocking of potentially compromised users.

Recommendations:

- Okta. Considered the gold standard for Identity Management, they're slightly more expensive than other solutions but best in class in defending users.
- **Secondary recommendation:** Duo. Now owned by Cisco, Duo is considered a major player in the Identity Management however its user awareness and threat identification isn't as robust as Okta.

DARK WEB MONITORING: THE CANARY IN THE COALMINE

With the explosion of stolen or leaked usernames and passwords in the Dark Web, the world has seen a multitude of massive cyber-attacks successfully launched thanks to a single username and password. Colonial Pipeline was shutdown after an attacker got a hold of a username and password in the Dark Web and used it to log into their billing system. Add to this that many companies do not realize that their users are logging into multiple personal websites (think Amazon or Netflix or Facebook) using their company email address as a user since it's easier for them, and the attack scope widens to any third-party website your employees use.

Dark Web monitoring gives the organization the ability to identify stolen credentials as soon as they are discovered for sale or for free download in Dark Web identity theft forums. It's the quickest way to understand what data is out there and then to change passwords or logins hopefully faster than the criminals can login.

IMPORTANT

Dark web monitoring gives the organization the ability to notice stolen information as soon as they are discovered for sale on the dark web.

Recommendations:

- Security Fanatics has a Dark Web monitoring solution combines multiple sources and Identity Theft forums to ensure the fastest turnaround of potentially exposed credentials.
- **Secondary recommendation:** Breach Secure Now is another solid option though only incorporates their own research into their results.

PASSWORD MANAGEMENT: KEEPING LOGIN PASSWORDS RANDOM AND SECURE

Dovetailing with Dark Web monitoring is password management, a centralized way to manage and secure passwords for an organization.

A good password management solution has the following characteristics:

- Encryption of the application and storage of passwords so a stolen password manager cannot be accessed.
- Multifactor Authentication that ties into an organization's Identity Management solution.
- Password generator to ensure that passwords are not reused.
- Anti-tampering for mobile apps that will self lock when they sensed they have been cloned.
- Customer cloud infrastructure that is running containerized military grade encryption so the password management company and attackers cannot access the password database without authorization

Recommendations:

- 1Password. Rating best in class after numerous tests, this manager meets multiple security compliance standards.
- **Secondary recommendation:** Dashlane. This platform has excellent integration for IT management of passwords however is not as hardened for security as 1Password is.

PENETRATION TESTING: REGULARLY VERIFYING SECURITY

Penetration Testing an organization to ensure that its public facing assets such as a website and office firewalls are properly configured, up to date, and able to mitigate attacks. Change management is also part of the equation here as many organizations may install or remove equipment regularly that requires changes to the public facing infrastructure. Finally, compliance standards such as PCI and CMMC also require quarterly penetration testing to ensure compliance.

Recommendations:

- Security Fanatics. They offer comprehensive penetration testing for compliance and change management using both NIST, ISO and CIS standards.
- Optiv. Another leader in this area though rather expensive to use.

EMPLOYEE EDUCATION: THE MOST IMPORTANT STEP

The best way to describe cyber security is this: You can build a Ferrari of a Cyberdefense System but if you hand over the keys to a chimpanzee, how far are you going to get?

The largest threat vector for hacking is humanity. If users don't have a filter to be wary and skeptical of data online then they become the weakest link in defense. Everything mentioned in this document is to wrap the user in protection, take choices for security away and move it to systems that will continuously monitor and defend them. Even with all of this, if they don't know that they shouldn't use free Wi-Fi or pickup the flash drive they randomly find then all the defenses in the world may not help.

IMPORTANT

The largest threat vector for hacking is humanity.

A good educational standard for a user should include but not be limited too:

- Understanding the philosophy of Zero Trust for their personal online lives. This will create a filter that they can use to screen out possible threats due to scams and infections.

- Understanding that the infrastructure around them when they leave their secured office is vulnerable and shouldn't be used. This includes free Wi-Fi, using other people's computers with their login information and more.

- Live testing the users without their knowledge for review and education. For example, there are services that will send the organization legitimate looking spam to see which users open it.

- Reinforcement periodically of this knowledge. Regular testing of users, as well as keeping Cyber-security education omnipresent in their lives will help ensure that they continue to embrace the Zero Trust mentality.

Recommendations:

- KnowBe4. Their motto is "Human error. Conquered." They offer comprehensive education and testing and are highly rated in terms of user satisfaction.
- Proofpoint Security Awareness Training, formerly Wombat Security, is considered the closest competitor to KnowBe4.

In the age of the Hacker, cyber-threats are virtually non-stop worldwide. In order to stay safe, online and in business, the cyber-defense strategy outlined here is the basic standard that all companies should be adopting when ensuring the confidentiality, integrity and availability of their data.

CONTRIBUTIONS

This article was made with expert advice and contributions of Nick Espinosa, Chief Security Fanatic and CIO of Security Fanatics, LLC. He is a contributing author of the book, Easy Prey, and host of a security based radio show in Chicago called The Deep Dive. For more information on the latest cyber-security threats, email him at nick@securityfanatics.com, follow him on twitter @NickAEsp or visit his Facebook page.