Certified Public Manager® Applied Research

Volume 2 | Issue 1 Article 5

7-27-2021

Steps in Building a Successful Resilient Cyber Protocol

Benny Yazdanpanahi

Follow this and additional works at: https://scholarworks.sfasu.edu/cpmar

 Part of the Library and Information Science Commons, and the Public Affairs, Public Policy and Public Administration Commons

Tell us how this article helped you.

Recommended Citation

Yazdanpanahi, Benny. . "Steps in Building a Successful Resilient Cyber Protocol." *Certified Public Manager® Applied Research* 2, (1). https://scholarworks.sfasu.edu/cpmar/vol2/iss1/5

This Article is brought to you for free and open access by the Journals at SFA ScholarWorks. It has been accepted for inclusion in Certified Public Manager® Applied Research by an authorized editor of SFA ScholarWorks. For more information, please contact cdsscholarworks@sfasu.edu.

Steps in Building a Successful Resilient Cyber Protocol

Benny Yazdanpanahi
Chief Information Officer, City of Tyler

Abstract

This article aims to help city administrators gain a systematic approach to building resilient cybersecurity protocols. Resilient protocols provide the basic organizational framework that layers employees, processes, and technologies that can address cyber risks to cities. Thus, these protocols provide the solid foundation necessary to protect cities and public institutions from the constant threat of cyberattacks. This article also offers suggestions on how cities can gain information technology (IT) resilience, and discusses boundaries in the layered approach to resilience.

Introduction

In computer-networking systems, resilience means maintaining and providing an adequate service level in the face of challenges to cities' regular operations. Resilience can be defined as the ability to recover quickly from complications or spring back into shape. Fast recovery from a corrupted system state is another example of resilience. The information technology (IT) community defines resilience as the combination of trustworthy, dependable, and secure operations that are tolerant of faults and disruptions in information traffic handling.

Today, many cities do not implement sound cybersecurity strategies despite increasing threats that may cause severe disruptions to their operations. The city leaders lack either a full alignment with IT workers or an understanding of the risks posed by cyberthreats and newly emerging technologies. In turn, they miss a golden opportunity to put cybersecurity and privacy at the center of their strategy. When not approached holistically, solutions often emerge as complicated, unsuitable, and difficult to manage.

Cities' employees are often one of the most significant cybersecurity risks. When they are well informed and trained, however, they can be the first line of defense. Additional investments in employee cybersecurity training—paired with secure architecture design—can significantly reduce an incident's potential severity. Cities must remain proactive and ensure that policies and strategies stay in place to quickly and effectively respond to and mitigate the risk in a cyberthreat event.

Cities must not layer their defenses with isolated solutions. Instead, they should integrate and automate their solutions to simplify the detection and elimination of threats. Experience has shown that implementing the correct architecture, developing the right processes, and training thoroughly and adequately solves eighty percent of the problem, a higher percentage than that achieved by new technologies alone.

IT disruptions such as ransomware attacks or even, as noted previously by the author in the IT news source GCN, a simple glitch, can knock out critical IT applications for several days and temporarily interrupt services.[1] These simple problems can create havoc amid cities' operations and interfere with service delivery, threatening mission-critical services such as protecting public safety and ensuring continuous water quality monitoring. To prevent these situations, resilience is the key.

Risks to Cities

Secure digital network design starts with the understanding that most cities' processes require cross-departmental communication using unreliable networks. While the internet unsurprisingly counts as an untrustworthy network, even cities' own internal network structures may be insecure. As a result, cities must anticipate that employees will access unauthorized information and must be prepared for hackers to get into the system.

The risk to cities increases as workers become more dependent on the internet to conduct cities' day-to-day operations, and the cost of cyber-crime increases tremendously with this change. According to the FBI's latest annual Internet Crime Report, cybercrime costs industries billions of dollars annually: "in 2019, IC3 received a total of 467,361 complaints with reported losses exceeding $3.5 billion."[2] Furthermore, cybercrime damages are projected to hit $6 trillion annually by 2021.[3]

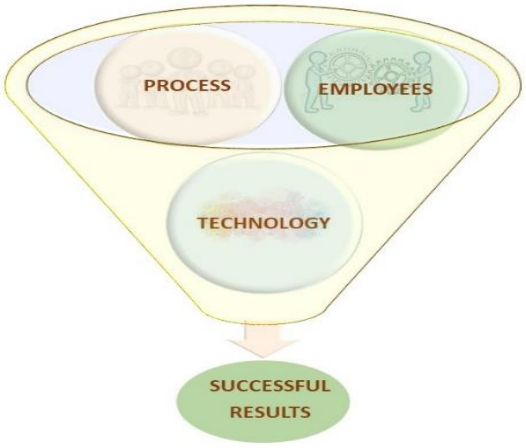
City administrators must protect their cities' digital infrastructure with a functional IT design focused on desktops, data centers, networks, artificial intelligence (AI), and cloud offerings. Administrators can accomplish this task by protecting personal computers (PCs) and laptops individually and breaking their city's network into smaller chunks by micro-segmenting the network through a switch or a firewall device. This micro-segmentation is called Virtual Lan (VLAN); it partitions and isolates a computer network at the second layer of the Open Systems Interconnection (OSI) data link layer model. In addition, cities can also use a Virtual Private Network (VPN) for remote access, Network Access Control (NAC) for user and system authentication, AI for behavioral analysis, and various cloud options for backup or failover.

These layered architectures add complexity, management difficulty, and costs to the cities' operating budget. As reported by a Gartner newsroom press release dated August 15, 2018, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019."[4] To eliminate downtime and reduce cost, it is best to adopt these technologies as early as possible. For cities to be resilient and practical, they need to evaluate how to leverage people, processes, and technology. Combining people and procedural techniques into a single integrated framework with security in mind produces an effective defense using technology.

Layered Environment

Cities should create a culture of cyber resilience that includes people, processes, and technology, using the Information Technology Infrastructure Library (ITIL) to create a layered, secure environment (See Figure 1). Figure 1 shows the successful transformation balance when employees perform a specific process or task using technology securely to achieve the city's desired results harmoniously.

Figure 1. Employees, Process, and Technology of the ITIL Framework



Employees

Employees can create substantial risks to cities' infrastructure when working with computers connected to the internet or bringing an unauthorized device, such as a USB flash drive, to work. However, when employees are well educated and trained, they can also be valuable and the first line of protection against cyberthreats.

Cybercriminals use various tactics to target employees who are not sufficiently trained and knowledgeable about cybersecurity. For instance, phishing emails designed to get employees to expose their personal information, such as their username and password, through a malicious website link are common. Employees tend to trust the sender and the validity of the messages they receive, so they click on links they should not. Unfortunately, by clicking, they put the city in danger. Cities must have consistent training classes and anti-phishing campaigns throughout the year to keep employees aware of possible schemes. City employees should know when they make their city vulnerable to cyberthreat. The goal must be to educate and train city employees to recognize the threat, report it, and then delete suspicious emails rather than clicking on the enclosed website link.

Training is vitally important because employees often fall victim to common emotional ploys used by cybercriminals. For example, according to Rosa Rowles, cybercriminals use the following emotions to get people to act without thinking:

> **Fear**: Malicious perpetrators use strong language to manipulate and convince victims that if they do not act quickly, there will be damaging consequences for them or their loved ones. For example, a perpetrator could claim that police will be issuing arrest warrants or that the user's bank account will be seized.
>
> **Greed**: Everyone enjoys getting something for free. So, cybercriminals trick phishing victims into action with the promise of getting a prize or monetary award.
>
> **Curiosity:** The attackers can entice the user by promising them something of interest to deceive them. This method could be as simple as an email stating that an unspecified

purchase the user made is ready to ship, and that they can click on a link to review their order.

Helpfulness: Most of us from a young age have been taught to be helpful. People are sometimes tricked by fake messages or emails from distant relatives seeking help using pleading or distressing language.[5]

Sometimes hackers fake emails from upper management to get users to react. The targeted employee is compelled to respond because the email looks like it is coming from someone with authority in the city. In addition, the targeted employee is not likely to question why they should send a wire transfer without checking the request's validity or provide confidential employee records to someone else.

In 2019, the State of Texas passed House Bill 3834 (HB-3834) and later House Bill 1118 (HB-1118), which required state and local government employees and state contractors to complete a cybersecurity training program certified by the state cybersecurity coordinator.[6] Cybersecurity training will create a strong security culture that can go a long way toward minimizing threats for city government, because employees will be aware of the tricks cybercriminals use and will routinely examine communications for those ploys.

Process

Cities must be proactive and ensure policies, procedures, and strategies are in place to quickly and effectively respond in a cyberthreat event. For example, cities must have incident response plans containing processes and operational approaches to address security breach incidents and to recover as quickly and efficiently as possible. In addition, ensuring backups are performed regularly and testing these backups is vital to reducing downtime and increasing data recovery from a potential security breach.

Cities must be proactive, update all systems' firmware and software, and monitor their systems to detect behavior indicative of cyberattacks. City administrators can better understand the landscape of cybercrimes by partnering with and subscribing to local and global threat monitoring tools.

The effective prioritization of assets is another necessary process. Cities must have a thorough knowledge of the location of their critical assets. These assets must be prioritized based on which would have the most significant impact on city operations if breached. Cities must develop policies and procedures and arrange strategies to keep data more secure; cities should reduce risks by implementing network segmentation and creating access control policies for specific sets of data.

Access control policies provide another method to improve core security. Such policies work using the principle of least privilege to ensure users can obtain authorization only to the pieces of information necessary to perform their jobs. This method reduces the risk of exposure and concerns of a data breach.

Technology

Cities should not rely upon implementing isolated solutions as they design their cybersecurity defenses. Instead, they must select tools that can be integrated and automated to

create a holistic approach that helps to detect and mitigate threats. In addition, cities must implement a mature cybersecurity program that is formal and optimized with a process model that focuses on being thorough, repeatable, and continuously improving.

Successful Results

For cybersecurity to be effective and successful, cities must think through how they leverage employees, processes, and technology to defend against today's threats; IT teams must take a layered approach to their cybersecurity and have various security controls in place to protect separate entryways. All these practices combined into an integrated framework strategy will yield the most effective defense against cybercrime.

Digital Resilience is Critical to City Operations Sustainability

As cities across the nation are forced to deliver more service with less staff, they must rely more on digital technology to provide valuable services to their citizens. As a result, the cities must increase their IT expenditure on digital technologies to transfer manual services to digital processes to achieve the desired results. These costs will include adopting public and cloud storage and implementing on-premise systems to connect substantial amounts of data. However, cities will be putting their daily operations at high risk if they are not prepared to protect their digital assets from an attacker or system malfunction, which risks can manifest in several ways:

Financial instability: When cities are hacked, employees cannot perform their daily tasks, especially if their work is highly dependent on ad-hoc access to data for retrieval or data updates. The average cost of downtime to cities can be massive, depending on the size of a citys' operations. This cost can be calculated per hour across the city—the direct and indirect losses in employee productivity and disruptions in service to citizens can be huge.

Ineffectiveness: While modernizing a city's operation and cloud initiatives, administrators must ensure that detailed data is available and accessible to all city employees and citizens at all times for better decision-making, delivery of services, and transparency to citizens. Data still needs to be securely available for city employees to use and analyze in real-time during any digital transformation. Without modern tools to protect and audit data integrity, many IT projects may not successfully enable cities to deliver the desired services to their citizens during completion and updates.

Distrust: Trust is necessary in a relationship between two parties conducting business together. As cities modernize their IT infrastructure, the citizens need to trust their city's online platform so that they can pay their water bills or traffic fines, apply for permits, or collaborate on sensitive client records. Citizens will lose trust quickly when a city does not protect their citizens' data and cannot recover after a cybersecurity disaster. Therefore, cities need to have an IT resilience strategy to maintain their services in the event of a cyber-attack.

Cities that do not test their backup strategy regularly could find themselves losing unrecoverable data. This can be easily avoided by periodically testing and restoring the backup

systems from on-premise backup tape or the cloud. IT resilience is unique to each city, depending on its size and budget. Remarkably, only a few cities so far have documented an enhanced IT resilience process, but they can get there.

How Cities Can Gain IT Resilience

City leadership acceptance of and investment in IT resilience processes, including increasing the IT budget for growing cloud adoption, will drive sustainability and resilience. However, cities' economic and political challenges may impede IT resilience sustainability. Therefore, city management and IT departments need to focus on IT resilience and the impact it will have on sustainability and service delivery by considering the following subjects:

Data availability and digital transformation gap analysis: IT should consider both a city's overall and each city department's individual operating environment processes, as well as the available technology to recover from planned and unplanned downtime. Many cities only restore or update individual files, not their entire data center. When cities go through a digital transformation, they need to anticipate data availability for their employees and constituents. Public cloud services such as Amazon and Microsoft Azure provide an example of technology which can be used during this shift. As service providers' continuity is widely distributed among different parties and more internal and external stakeholders are added to the mix, more application ownership is offloaded from IT onto each city department's operating units. These digital transformations are time-consuming and require coaching and training for city leadership to understand the difference between different applications' and services' data protection requirements. In addition, For IT resilience to be effective, many of the applications and services that each department manages must be integrated and operated under a single IT operation continuity plan. Finally, the other city departments' operation and IT budgets must be aligned for data availability during the city's digital transformation initiatives.

The importance of assessing the tools and services IT uses for sustainability and resiliency: Cities' IT departments need to change their approach and be open-minded by embracing hybrid and multi-cloud technology infrastructures in operations and data management security, end-to-end IT governance, and the skills of the technology staff. Knowledge of the cloud is vital to the future of resiliency initiatives as these initiatives ease deployment and integrate with various data sources, including other cloud applications and Infrastructure-as-a-Service (IaaS) platforms. Large municipalities can offer a hybrid cloud as an IaaS to neighboring cities in order to share resources and costs. IT departments should concentrate their efforts on leveraging on-premises and cloud solutions as an essential foundation of their IT resilience strategy, from both cost and functionality perspectives.

The fact that growing volumes of data create complexity, an opportunity for data analysis, and vulnerability: Many city governments have experienced malicious attacks in recent years, resulting in service, data, and productivity losses. Sophisticated ransomware, phishing, and malware sent by hackers provide a constant challenge for many cities. Stealing data and holding it for ransom is becoming increasingly profitable for attackers who target cities, as more cities begin to go through digital transformation or

begin to gather more data for analysis and real-time decision-making. As a result, cities must account for the value of protecting data from malicious attacks. As more data is distributed across and integrated into a city's workflows, more attack paths and more points of failure are apparent. An IT resiliency strategy must account for this while also considering data security and protection requirements.

As cities go through modernization and cloud initiatives, data must be available and accessible to city workers and citizens. Nevertheless, most cities still experience a considerable disruption associated with their data redundancy, transfer, migration, and recovery planning. Therefore, cities must address these challenges as a first step for the IT resilience plan. In addition, many cities are still on complex legacy systems, which dictate how and when cities can implement or migrate to modern tools needed to achieve IT resilience.

Cities need to position themselves for data protection, backup, and recovery as part of the operational transformation to meet many compliance regulations. As demand increases to access cities' resources from various sources, significant opportunities and incentives arise to automate and simplify the complex processes involved without putting much strain on IT budgets and staffing. Improving data protection automation and redundancy replication can help cities' return on investment. The adoption of cloud-based services is an excellent opportunity for cities to reduce their risks.

IT resilience is an emerging concept for many cities. Some cities have implemented some level of IT stability by protecting their data for availability and continuity. However, the IT resilience plan depends on the close collaboration between the city department operation units and IT on post-disaster planning to minimize downtime on data loss or operation recovery. To eliminate data loss while delivering continuous service and access to the city's digital assets requires the collaboration and coordination of people, processes, and technology.

Cities that will not embrace the cloud and modernization projects as a high priority will encounter disruptive events, unplanned downtime, and data loss. These impose a significant financial burden and negatively impact a city's ability to deliver service to its citizens on time. Conversely, protecting a city's digital assets with marginal disruption will simplify the people, processes, and technology requirements necessary to succeed.

How to Set Boundaries Using a Layered Approach to Resiliency

Potential cybersecurity risks can happen at different levels, so several layers of defense against these cyberthreats are necessary. When organizations or individuals connect to an outside network like the internet or other government or non-government entities, they should not be surprised if they experience service interruption attacks. Instead, they should anticipate at some point that they will come across a security breach problem. Therefore, the best defense is being vigilant, thoughtful, and proactive, and layering protection. Using a multi-layered approach, cities can ensure that an attacker who infiltrates one network layer will not penetrate other network layers.

A city's initiated security strategy must include measures that protect all layers of the infrastructure model. Generally, cities need to have plans in place for all security level models, from the basic to the more complex security levels.

Desktop Security

The first line of security on cities' networks must protect the user's endpoint desktop or laptop. Many malware or virus outbreaks can be stopped by implementing the proper security policies on these computers.

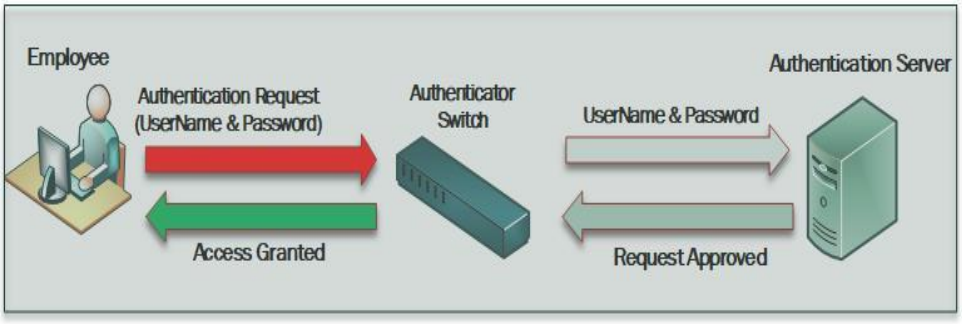
Desktop security within a city network is managed mainly by the IT department from a central server with applied group and access control policies. When a user on a desktop system logs on to their computer, the domain controller server dictates the policies that control that computer's activities on the network. This method delivers centralized control that makes managing large desktop network systems in the city much easier.

Cities must use antimalware and antivirus software to protect their network systems from phishing, spyware, trojans, malware, and viruses. Malware can spread quickly into the network infrastructure and spring attacks, causing the systems to malfunction.

Network Security

Implementing Network Access Control (NAC) regulates which individuals can access a city's system and network and which ones cannot. It allows the city to identify different users and devices and determine when authorized or unauthorized employees can or cannot access the system. The city can, therefore, enforce different security policies, such as automatically verifying user identity before allowing physical network access, as depicted in Figure 2. More specifically, Figure 2 illustrates how an employee gets authenticated by providing their username and password to an authenticator switch with NAC software to ensure the user device and the credentials are valid and are domain-joined. Then the username and password are sent to the authentication server for verification and access to the network, server, and software. After the request is verified, the permission passes back through to allow the employee to log in and gain access to the allowed city information system. A NAC is not a total guarantee; it is just another layer of protection against a rogue device or an intruder.

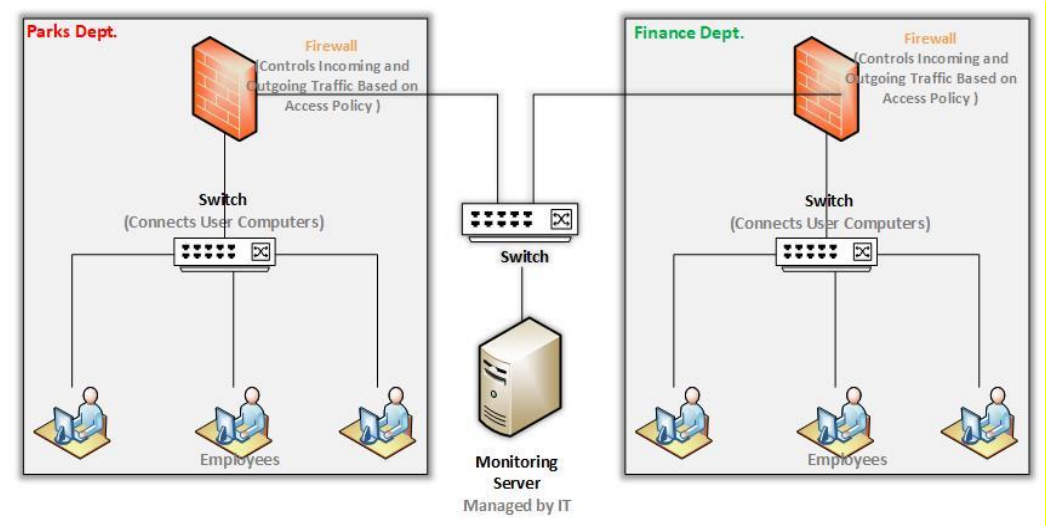
Figure 2. Network Access Control



In today's current cyberthreat environment, cities must consider that they will most likely have a security breach at some point in time. Implementing a segmented network that divides a network into multiple smaller networks makes it more challenging for a cybercriminal to penetrate and launch an attack against the entire network. It also creates an obstacle for insiders, as it can isolate sensitive data and systems from internal snoopers and prying eyes.

As depicted in Figure 3 below, segmenting or subdividing the networks into smaller pieces controls how traffic flows from one network segment to the next. For example, the city security policy outlined below uses firewalls that control incoming and outgoing network traffic from each department based on preset security rules to restrict parks employees from accessing the finance department's financial journal entry or reporting system. Segmentation can slow an attacker or an unauthorized user as they try to move across the systems. Still, unfortunately, it does not stop the attacker from doing damage. A segmented network still has to be monitored by the IT system administrator using security monitoring software on a server to ensureproper operation. Cities should provide an adequate budget for monitoring all devices and assets such as servers, PCs, switches that connect these devices, and the city's enterprise software as part of the network build-out. The goal is for the IT system and security administrators to catch network traffic abnormalities at every level of operation.

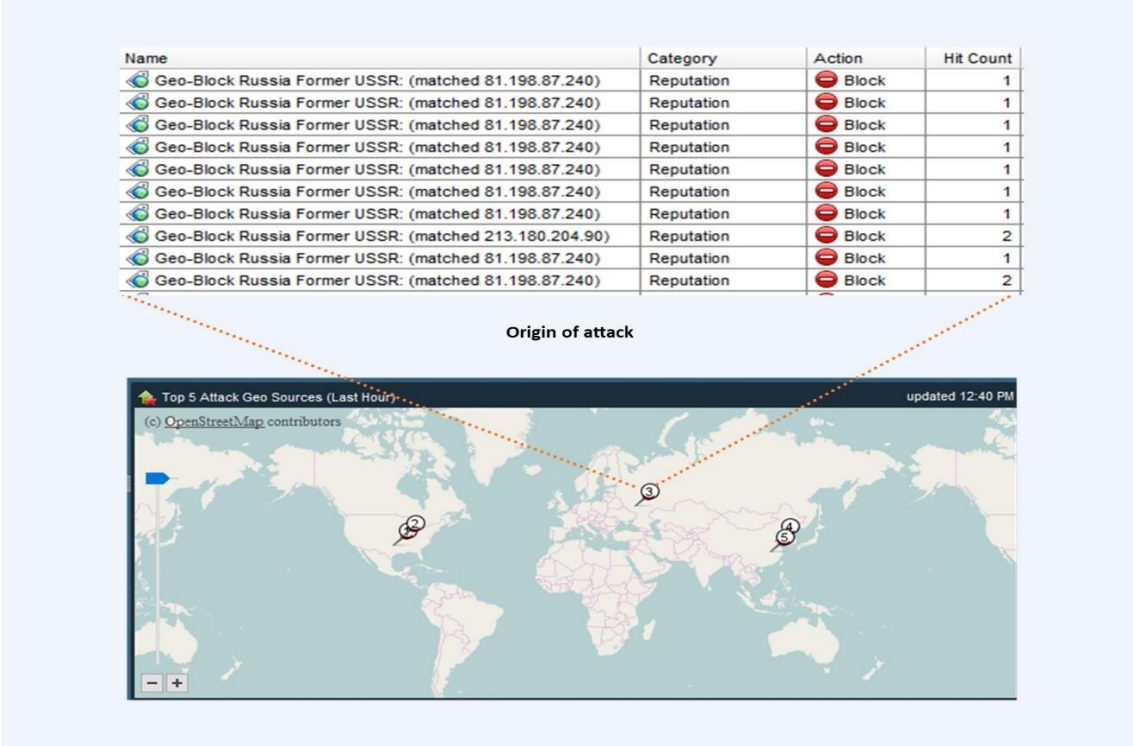
Figure 3. Network Segmentation



Many cities have implemented a firewall security device that monitors incoming and outgoing network traffic based on a defined security policy or rules for detecting attacks. Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are tools that cities can use to monitor traffic coming in and out of their networks and to pinpoint the source of attacks. For example, as depicted in Figure 4, many attacks (Hit Counts) are initiated from geographically blocked countries like Russia. These attacks are being blocked based on the pictured city's adopted geo security policy (See Figure 4).[7] However, suppose someone gets through the network infrastructure, and the attack was not mitigated. In that case, most investigator tools do not look at what is going on inside the network, and the unwelcome guest will have free range to perform the desired attack.

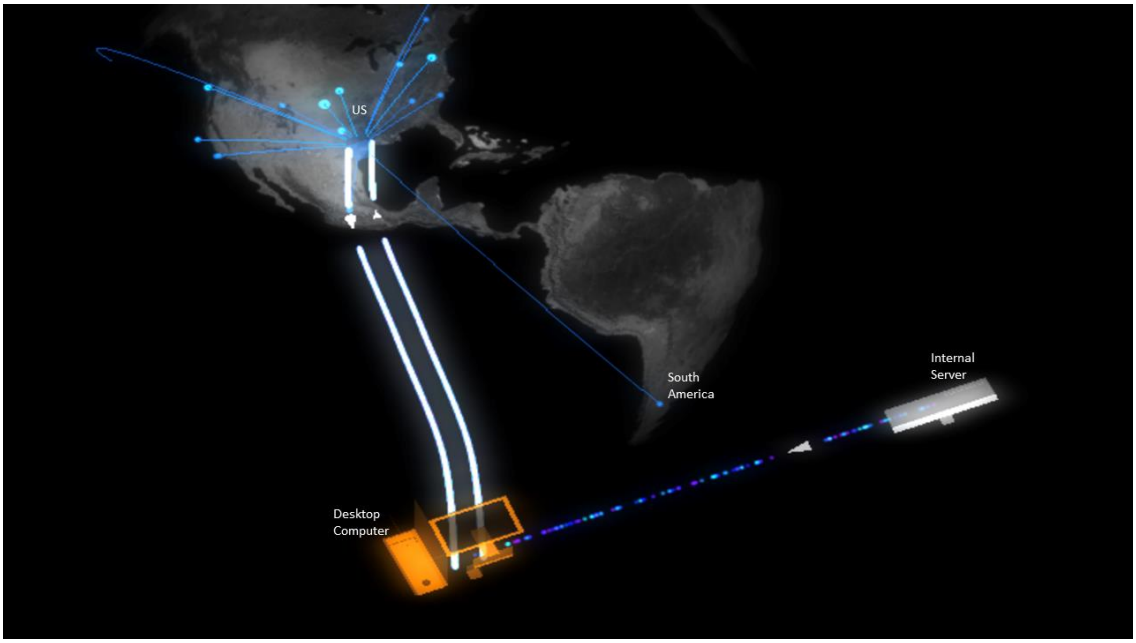
While easy to manage, a flat network infrastructure provides an excellent opportunity for malicious attacks. Therefore, micro-segmentation is recommended for the sake of resiliency.

Figure 4. Sample IPS in Action



Self-learning behavioral analytic appliances help identify abnormal behavior on a network by notifying the IT security team when someone acts abnormally on the system. For example, a self-learning cybersecurity AI such as Darktrace uses predictive machine learning to detect Digital Network Architecture (DNA) and neutralize threats without human intervention. It works by analyzing the nature of an event, starting with a source device. Devices exhibiting anomalous behavior are color-coded to signify such activity and centered within a visualizer to assist a security team in determining devices that were caught being connected to the system and external endpoints as outlined by their geographical location on a world map view. In Figure 5, in the bottom center of the picture, we can see a computer colored orange to signify that there has been anomalous activity detected. The computer also shows as being connected to another internal device, specifically an internal server. On the world map in the background, many connections are being made across the US, and at least one connection in South America (See Figure 5).[8] In addition, AI learning model systems must be trained to test various defense strategies to stop the spread of malware or viruses during a cyberattack by eliminating the infection and the root cause.

Figure 5. Screenshot of Darktrace AI in Action



When a city connects its network to the internet, it needs to ensure it has adequate network security protection to protect its internal network infrastructure from an intrusion. For inbound and outbound traffic, a firewall is a standard device that provides network security; however, a firewall alone will not suffice. Adjustments need to be made to other parts of the city's systems as well.

Application Security

Application-level security controls the interface between an application and users; these security measures can monitor how a client accesses the server and security exposure. Depending on how clients access the server, applications and services can be exposed to security exploitation by unauthorized users.

System Security

The last line of protection against intrusion must be system security. Consequently, the first step in a comprehensive internet security strategy would accurately configure basic system security on individual network computer systems.

Data Transmission Security

The internet has made it much easier to transfer data from one medium to another. As a result, it has become a prevalent part of our daily life. However, information often is not securely transferred to our anticipated receivers when using the internet. For example, when transmitting data across an open and untrusted network, such as two separate city offices that need to be connected via the internet, we must control the traffic traversing from source to destination, because the data travels through several different telecommunication environments which cannot

be controlled. In this case, it is better to configure an application to use a Secure Socket Layer (SSL) or Virtual Private Network (VPN) software such as NetMotion for remote users to transfer data; otherwise, the data will travel through the internet unencrypted and can be available for anyone to intercept, view, and use.

The city's internet security policy must include a data transmission strategy to protect data as it crosses the internet. Many solutions and tools need to be addressed in the policy, such as email encryption, website encryption, Secure File Transfer Protocol (SFTP), and cloud services.

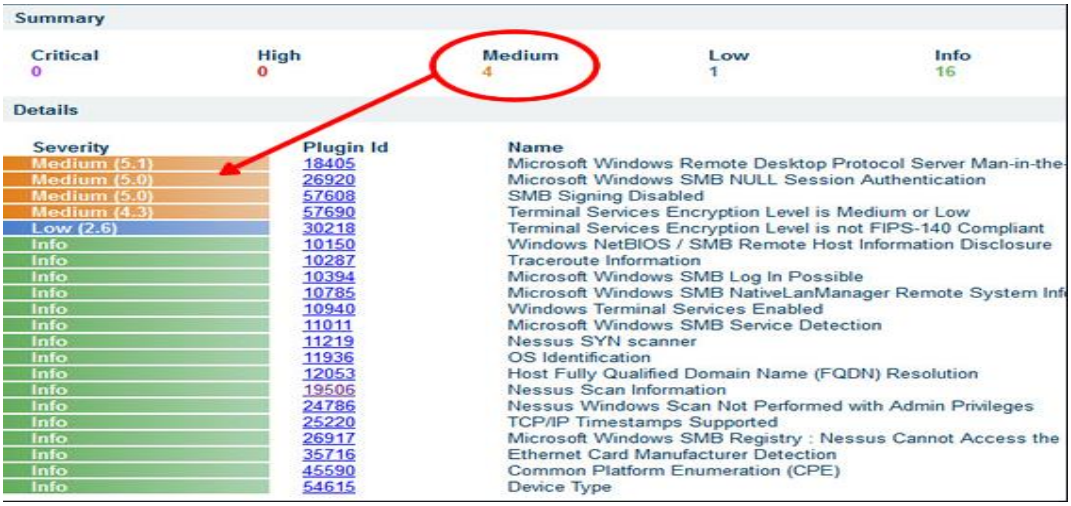
Vendor Access Control

Often, third-party vendors need privileged access to a city's network to correct a software code that impacts operational services. However, giving access should not mean relinquishing control of the IT security environment to the vendor. This act has been vastly exploited in the past by hackers when the access controls were left unattended. Instead, access control is best maintained by keeping a log of when, to whom, and by whom access was granted for each application. For example, an administrator should record a connected vendor's tech support name and phone number, when the connection was closed, and by whom it was opened. A Service Level Agreement (SLA) with specifications for this security policy should be included in the contract with each vendor.

Vulnerability Scanning

Devices on the network may need continuous scanning for vulnerabilities, compliance, and rogue activities. Various scanners on the market, such as Qualys, Nessus, and Nexpose, can scan devices and explain why a device failed or malfunctioned and how to fix the issue.[9] Figure 6 displays Nessus listing the severity of the vulnerability category for each issue listed (Critical, High, Medium, and Low), and explaining what kind of vulnerability exists under the name column. Nessus will also explain what actions need to be taken.

Figure 6: Screenshot of Nessus in Action



Regulatory Compliance

Many cities must adhere to and abide by specific regulations, such as the regulations of the Criminal Justice Information System (CJIS), Purchasing Card Industry (PCI), and Health Insurance Portability and Accountability Act (HIPAA). In such circumstances, it might be better to have each regulated system in its own controlled and monitored environment. [10]

Data Center Redundancy

Minimizing computer downtime must be a top priority for every city that is providing services. Developing a strategy to work with a colocation data center is a smart move and can be highly cost-effective to protect cities' digital infrastructure systems from unexpected downtime. These colocation data centers need to have redundant power, cooling, and connectivity, in order for partnerships with them to be worthwhile.

Incident Response

Cities need to focus on a methodical, structured resilience strategy for providing defense, detection, remediation, recovery, diagnosis, and refinement to reduce the impact of costly service disruptions. For example, when dealing with an incident, an extra layer of monitoring identifies an attack more easily and contains the threat before the attacker can do more damage.

Once the cyberthreat has been isolated, the response team can eliminate the risk in an isolated network environment. Once the threat has been eradicated from the affected department operation unit, that unit can return to productivity. After the incident, all security response team stakeholders need to meet and discuss lessons learned and what processes need to be improved.[11] Engaging the department operation units by reviewing security and resilience plans and revisiting and updating the plan list as new systems are implemented into the city operating environment is vital. IT resilience does not offer a quick fix; it is a journey that the whole city must take together.

Industry Trends

The IT world is evolving daily; rapidly changing technology allows cities to provision and de-provision resources to fit their operating environment needs. Emerging technologies, such as virtual applications, servers, storage, and networks, will boost efficiency, agility, scalability, and workload ability while reducing IT expenses.[12]

Conclusions

Many city networks receive frequent attacks from multiple directions. In addition, the cost of failure significantly increases as the demand for instant access to information via the internet expands. There are many resiliency approaches, from fault-tolerant applications to network segmentation, cloud, and multilayer security. However, cities are still vulnerable to environmental threats and human error.

The city must protect itself by using a systematic approach to defense. Cyber resiliency is not a replacement for cybersecurity; these systems must work together to predict and respond effectively to attacks. Cyber resiliency mainly concerns continuing operations during recovery.

Many systematic approaches together can thwart an attack. However, there is no single correct answer as to how much cyber resiliency protocol is enough. It all depends on how much risk a city is willing to take based on its mission and operational goals. The right combination will build a city's resiliency against cyberthreats.

Notes

---

[1] Benny Yazdanpanahi, "How One Texas Town Built IT Resilience," GCN, October 4, 2019, accessed September 11, 2020, https://gcn.com/articles/2019/10/03/tyler-texas-disaster-recovery-resilience.
[2] *2019 Internet Crime Report*. Federal Bureau of Investigation, Internet Crime Complaint Center, February 11, 2020, accessed 13, 2020, https://pdf.ic3.gov/2019_IC3Report.pdf.
[3] Steve Morgan, "Cybercrime Damages $6 Trillion by 2021," Cybercrime Magazine, October 16, 2017, accessed September 13, 2020, https://cybersecurityventures.com/annual-cybercrime-report-2017/.
[4] Susan Moore and Emma Keen, ed., "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," Gartner, Aug 15, 2018, accessed September 13, 2020, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.
[5] Rosa Rowles, "Emotions Used in Human Hacking," Security Boulevard, March 3, 2021, accessed May 3, 2021, https://securityboulevard.com/2021/03/emotions-used-in-human-hacking.
[6] Giovani Capriglione, *Texas Senate House Bill 3834*. Effective June 14, 2019, accessed September 13, 2020,https://capitol.texas.gov/BillLookup/History.aspx?LegSess=86R&Bill=HB3834.
[7] "Tipping Point Threat Protection System: Go Beyond Next-Gen IPS Without Compromising Security or Performance," Trend Micro, March 2021, https://www.trendmicro.com/en_us/business/products/network/intrusion-prevention/tipping-point-threat-protection-system.html.
[8] "Cyber AI," DarkTrace, 2021, https://www.darktrace.com/en/cyber-ai/.
[9] "The Nessus Family," Tenable, 2021, https://www.tenable.com/products/nessus.
[10] Ben Rothke and David Mundhenk, "A Guide to Practical PCI Compliance," Network World, November 16, 2007, accessed September 18, 2020, https://www.networkworld.com/article/2288753/a-guide-to-practical-pci-compliance.html.
[11] Allyson Vicars and Emie Hood, "An Introduction to the SANS Institute's PICERL Approach," Advisory Board, November 2016, accessed September 21, 2020, https://www.advisory.com/-/media/Advisory-com/Research/ITSC/Research-Notes/2016/Ransomware-Incident-Response.pdf.
[12] Mora Gozani, *Network Virtualization For Dummies®,* VMware special ed. (Hoboken, NJ: John Wiley & Sons, 2016), accessed September 21, 2020, https://microage.com/wp-content/uploads/2016/12/Network-Virtualization-For-Dummies.pdf.