CYBERSECURITY

You are more at risk than you think.

April, 2018

The question is no longer if you will face a massive Cyberattack, but when - and to what extent. How prepared are you?

A COMPLEX PROBLEM

Customers today engage with your brand in a variety of ways. They connect at any point, from any device (web, mobile and wearables) at any location. In order to deliver an exceptional customer experience, meet order demands, deliver sensitive personalized content and address scalable computing needs, you need a web of internally developed partner and vendor solutions.

Managing a business forces you to rely on critical systems that run on private servers, shared cloud infrastructures or third-party Software as a Service (SaaS) platforms. The supporting technology infrastructure for these systems has also evolved from on premise to the Cloud, leveraging services and technologies that often reside in data centers across the globe and are managed by third-party service providers.

The Bring Your Own Device (BYOD) trend has enabled employees to access critical corporate resources, while using the same device at any number of public locations to check their social media accounts and personal emails.

THE POTENTIAL OF A CYBERATTACK

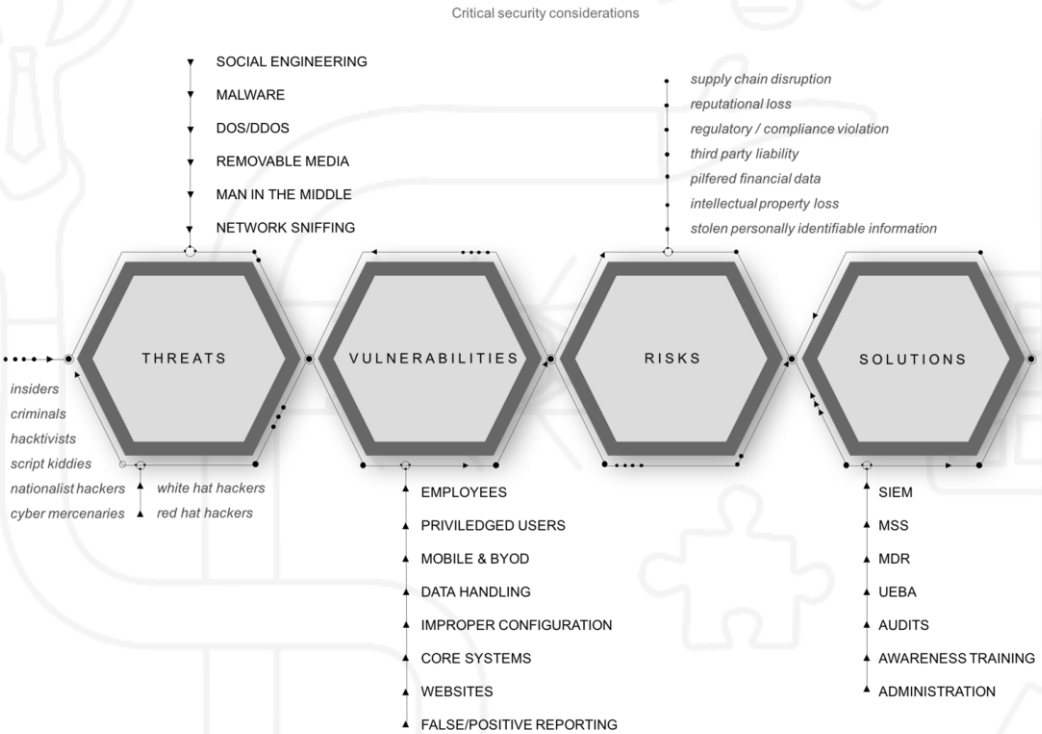
Companies invest significant resources to protect critical corporate data against the potential of a cyberattack. A number of end-point solutions (i.e., firewalls), encryption methods and Identity Access Management (IAM) policies are usually implemented as precautionary measures.

Some businesses go even further by deploying state-of-the-art intrusion detection and monitoring solutions. They've also defined and implemented a host of user authentication procedures to ensure the legitimacy of trusted users, their activities and geolocation. Finally, to ensure oversight, businesses employ security engineers, internal auditors and Chief Security Officers (CSOs) to ensure adherence to key cybersecurity standards such as:

- Open-Enterprise Security Architecture (O-ESA)
- NIST 800-53
- Center of Internet Security (CIS) Top 20
- COBIT
- ISO27001/2

Even with all of the cybersecurity measures available today, the number of cyberattacks and breaches increases daily. Cases of exposure, theft of critical corporate (or customer) data, system wide outages, pilfered financial data and increased exposure to Ransomware are continuing to rise.

Considering all these factors, you are more at risk of a Cyberattack than you may have thought. We highlight critical cybersecurity risks and demystify solutions that your company can adopt to improve your security posture and minimize your risk of a cyberattack (or worse - a cyber doomsday scenario). We identify key security management considerations by analyzing the vulnerabilities, threats, risks, and solutions.



UNDERSTANDING THE VULNERABILITIES

Cyberattacks are usually driven by profit (rewards, bounties), malice (disgruntled employees, angry customers), or corporate espionage. To achieve their objectives, cybercriminals undertake a range of tactics aimed at exploiting vulnerabilities.

"62% of security breaches are from insiders who have valid authentication credentials, access to critical data/assets or have privileged access."

A. Your Employees

More often than not, cyberattacks are perpetrated from inside the network by employees who have access to critical systems (or manage sensitive data). Cyber attackers seek out these employees as their primary target. The goal is to grab critical user credentials through seemingly harmless phishing expeditions.

Once a user's credentials are compromised, the attacker takes over the account, expands its footprint and proceeds to attack critical company resources. User and Entity Behavior Analytics (UEBA) solutions can unmask these imposters by baselining and continuously analyzing user behavior.

Monitoring suspicious employee behavior and attempts to access non-authorized systems can help minimize the risk of data theft, fraud, sabotage and policy violations.

B. Privileged Users

Privileged users are at a greater risk. Administrative root privileges or permissions establish critical access rights such as:

- Who is allowed to read and write files?
- Who can manage directory attributes?
- Who can execute programs?
- Who can perform sensitive administrative level operations?

An application running with root privileges can access everything and change anything. Cybercriminals diligently seek out privileged user credentials to gain access to critical system resources and execute malicious software and data extraction routines.

C. Mobile & BYOD

The explosion of BYOD combined with the popularity of mobile apps that can potentially carry malware also create a significant vulnerability for your business data. Users who administer their own devices typically apply limited diligence in patching or deleting unused apps which can enable attackers to exploit known vulnerabilities.

These mobile users have banking, credit card and other financial apps installed on their device. Downloading apps (in particular those from unrecognized third-party app stores) or failing to properly patch apps (with known vulnerabilities) creates a huge risk.

Not only does the user risk exposing Personally Identifiable Information (PII), but cybercriminals can use these apps to turn the mobile device into a discovery bot once the device is connected to the corporate network (Wi-Fi).

D. Data Handling & Exposure
Policies that govern the handling of sensitive data (at rest or in flight) are critical for protecting this data against unauthorized exposure. Cyber attackers typically use malware to intercept data between a server and the browser with a Man-In-The-Middle attack (or by manipulating a web application).

The goal is to access sensitive or PII information (like credit card data). As a rule of thumb, businesses should encrypt as much data as possible (at every stage) to ensure protection.

E. Improper Security Configuration
This is one of the most common (and most dangerous) vulnerabilities. Cyber attackers easily scan and discover vulnerable web servers and applications that have been misconfigured (or simply use default settings). Known security vulnerabilities that are not properly patched can expose critical systems to diligent cyber attackers.

F. Core Systems
Critical security infrastructure components such as servers, networks, endpoint security devices and core systems (custom developed or off-the-shelf ERP systems) are also vulnerable to attacks. Cyber attackers can apply a number of tactics such as buffer overflows and code injection to gain access, corrupt critical data, crash programs or execute hidden malicious code.

As is the case with improper configuration and patching, security administrators should be held accountable for ensuring that proper patch levels are in line with vendor recommendations.

G. Websites
Multitier websites that fail to apply proper validation (certificate pinning) or have broken authentication and session management policies can create a vulnerability by redirecting users to other pages and websites.

Attackers seek out this vulnerability to gain access to PII data (i.e., accounts, passwords, session IDs) or redirect unsuspecting users to phishing or malware sites.

H. Reporting
Security programs can gather unprecedented amounts of data about threats and attacks. However, correlating and analyzing a cumulative wealth of information creates an additional vulnerability.

Managing and analyzing false positives often creates the risk that real problems are masked amidst a wealth of data identified as unusual or malicious. False positives also cause the security staff to be distracted from dealing with legitimate security threats - real threats and alerts could be buried in a mountain of false positives resulting in a major risk.

THE THREATS

A threat is a known activity that exploits a company's vulnerabilities in order to breach their security fabric and gain unauthorized access to its systems and data. The list of possible security threats is extensive. Below are some of the most common types of threats. (This list is by no means comprehensive.)

A. Social Engineering
Most modern day attacks aim at manipulating unsuspecting insiders into handing over sensitive access credentials to networks, hosts or critical information assets. The attackers use psychology to illicitly compromise security.

"Most of today's cyberattacks are characterized by modern-day phishing scams and various forms of social engineering that successfully manipulate unsuspecting insiders."

"Most of today's cyberattacks are characterized by modern-day phishing scams and various forms of social engineering that successfully manipulate unsuspecting insiders."

Phishing is one of the most common techniques used by cyber attackers. However, attackers often combine leaked and publicly-available data with cybersecurity vulnerabilities to create more sophisticated attacks. Social engineering attacks don't rely on technology or protocols to succeed, but instead manipulate human psychology.

B. Malware
Malware is any program or file that causes a system to become inoperative or creates vulnerabilities. These programs perform a variety of functions, including but not limited to: pilfering, encrypting or deleting sensitive data and altering system functions.

Some typical malware threats include Ransomware (i.e., Wannacry), Viruses, Trojan Horses and Worms.

Ransomware - Attackers aim to prevent or limit users from using their own system. These attacks are primarily carried out for money - attackers effectively hold your computer hostage until you pay to release your system. You usually have to make the payment through Bitcoin or other obscure payment platform within a limited time period. Ransomware is commonly downloaded by unsuspecting users who visit a compromised website. It can also be distributed through spam email or other malware. The effects of Ransomware on the company can be crippling.

Virus - Computer viruses can cause critical programs to stop working. There are over 80,000 known viruses. The best defense is to implement an enterprise-wide anti-virus software solution (i.e., McAffee, Symantec, Sophos) and ensure signature files are continuously updated.

Trojan Horses - Attackers trick unsuspecting users to install malicious programs by delivering a payload through an inconspicuous email attachment or an app. Often, the user is unaware that he/she has downloaded a Trojan Horse until security scanning software detects its presence. The best defense is maintaining servers and computers up to date with latest security patches.

Worms - These use networks to replicate their existence into other computers. Cyber attackers typically use worms to disrupt their target's networking infrastructure. Like viruses and Trojan Horses, the best defense is maintaining servers and computers up to date with latest security patches.

C. DOS/DDOS Attacks

A denial of service (DoS) or **distributed denial of service (DDOS)** attack floods critical computing and networking resources with a steady stream of trash data. DOS attacks typically mask a larger attack. Once a user's computer or host is blocked by a DoS or DDoS attack, the attacker attempts to grab critical authentication credentials or sensitive data.

Often, the user is unaware that critical data is being hijacked until it's too late. DoS attacks can cause significant disruption to an institution's normal operations by interrupting the execution of critical systems.

DDoS attacks occur when multiple methods are used to flood multiple networking resources. To protect themselves, companies should deploy a combination of on-premise and cloud-based solutions to handle various attacks.

Because of the massive disruption that can be caused by DDoS attacks, a company should consider leveraging the services of a third-party, typically the core network provider or a managed security service provider (MSSP) to help proactively identify attacks and enable dynamic rerouting of network traffic.

D. Removable Media

Removable media is anything that can be brought into an organization and connected to a computer. Such devices include: USB stick, smartphones, tablets and wearables. Using removable media can pose a significant threat as the device may contain malware that downloads sensitive data or forwards this to an obscure internet site. Specialized software can help prevent the use of removable media and/or encrypt its content.

F. Man-in-the-Middle
A man-in-the-middle attack occurs when an attacker is able to position him or herself between two connecting end-points. This threat can be easily addressed by forcing strong authentication through adopting key security protocols such as IPSec/L2TP with endpoint tunnel authentication.

G. Network Sniffing
Network sniffing occurs when an attacker uses a protocol analyzer to inspect data at a packet level. The attacker may be able to inspect IP addresses, unencrypted passwords, sensitive data and MAC addresses.

After a vulnerability is discovered, the attacker begins an active attack. The best defense is to block packet analyzer activity on a network (except when legitimate support activities are required to troubleshoot a network error and only by a trusted network administrator).

The presence of a network sniffer or packet analyzer can be easily detected with the proper monitoring tools (see "Solutions" section).

THE RISKS

Managing risk is the fiduciary duty of top management, board members and officers. Management is responsible for ensuring proper steps are taken to prevent cyberattacks and protecting the company against data loss and disruptions that could ultimately result in significant financial losses.

Key risks resulting from cyberattacks include (but are not limited to):

Regulatory / Compliance Violations: Cyberattacks can result in a number of compliance law violations such as: Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and the Sarbanes-Oxley Act (SOX). Compliance law violations can result in significant fines, a decline in customer confidence and ultimately impact shareholder value.

Supply Chain Disruption: Disruption at key integration points across a company's supply chain can cause huge customer satisfaction problems and product delivery challenges. Disruptions can also cause massive problems in material resource planning and inventory management. This ultimately impacts customer satisfaction and the overall brand experience.

Reputational Risk: Aside from the costs associated with containing an attack (and managing the crisis, investigating the breach, paying for forensics analysis, compensating customers, replacing damaged systems and paying for lawsuits or penalties) a company is typically faced with a significant reputation loss. This reputation loss is even greater when personally identifiable information (PII) data is exposed.

Third-Party Liability: Cyberattacks and breaches also result in third-party liabilities and lawsuits, particularly when it can be proven that a lack of diligence resulted in a successful cyberattack.

Pilfered Financial Data: Unauthorized withdrawals from accounts or charges against credit lines are also a major risk.

Intellectual Property Loss: Loss of intellectual capital/property, nonpublic internal data and internal operational details can severely impact the company's ability to compete or deliver a differentiating value.

Stolen Personally Identifiable Information (PII): This includes any information that can specifically identify an individual, like social-security numbers, addresses, phone numbers, and email addresses.

SOLUTIONS

A number of security strategies can be adopted to ensure a reasonable level of threat defense. Several solutions are analyzed here. (The solutions identified are by no means comprehensive.)

"Crafting a solution strategy and architecture should be guided by a clear understanding of the organization's technical competence, strengths, weaknesses and compliance requirements."

SIEM (Security Intrusion & Event Management): Specialized tools can provide large enterprises with comprehensive solutions to help analyze event data in real time and detect cyberattacks and data breaches sooner rather than later.

SIEM tools offer dashboards, correlation models, searches and reports to support real-time security monitoring, alerting, incident response and compliance reporting. SIEM tools can be deployed on premises or in public, private and hybrid clouds.

Pros: SIEM tools provide extensive monitoring and reporting. They also greatly expedite incident response.

Cons: These tools typically require a dedicated staff to monitor reporting on a 24/7 basis. A basic Security Operations Center (SOC) structure is required to manage the tools and effectively sort through various event data.

MSS (Managed Security Services): To address the need for significant investments in retaining a qualified security staff, many businesses outsource their intrusion and event management operations to a Managed Security Service Provider (MSSP). Third party providers can offer extensive SIEM and compliance services on a subscription basis.

Pros: Deployment is easier as external infrastructure, staff and processes are leveraged - there is limited upfront investment.

Cons: MSSPs may have limited view into the organization's functions. While threat detection is swift, it can be challenging to effectively understand and map out an institution's security posture, proactively identify security gaps and provide post-incident remediation.

MDR (Managed Detection & Response): In order to address some of the gaps in traditional MSS offerings, many service providers are evolving to deliver more proactive MDR solutions. Rather than just monitoring and reporting, MSSPs enhance their services by delivering a suite of appliances that reside within the customer's environment to curate collected data (from the appliance combined with data from customer's security devices) and feed the data into an advanced threat intelligence and data analytics system.

MDR services monitor source content from networks, emails and various customer ecosystem endpoints to better detect, analyze and deliver proactive threat intelligence as well as structure appropriate responses to mitigate future attacks. Specialized dashboards provide direct customer insights into events.

The MSSP then delivers more detailed context and recommendations to the customer to ensure rapid containment and remediation of cyberattacks. Services are delivered on a subscription basis, while emergency remediation retainers are offered on an incident basis.

A number of MDR-specific solutions are also available (i.e., Arctic Wolf Networks, FireEye, Netwatcher). MDR providers leverage big data analytics platforms (i.e., Hadoop, Elastic database and NoSQL) that use curated security data to perform real-time threat detection, machine learning and analytics to deliver higher-fidelity threat intelligence.

UEBA (User & Event Behavior Analytics): UEBA solutions look at patterns of suspect human and machine behavior, then subsequently apply algorithms and statistical analysis to analyze anomalies and identify threats. UEBA brings machine learning and real-time analytics to security monitoring.

The goal is to protect against both external cyberattacks that have compromised a user's account and insider threats that originate from ill-intended users by analyzing user or system behavior.

For example, it may be suspect if a trusted user shows unusual attempts to access critical systems, data or hosts. It would also be suspect if a user/system is abnormally attempting to access certain network links or protocols (i.e., FTP, SMTP, HTTPS).

Big data platforms are used to analyze large volumes of user behavior encoding data to detect threats. Some level of machine learning is also incorporated to establish basic baseline behavior or a user fingerprint, then automatically differentiate this from anomalies.

Audits & Penetration Testing: Performed by certified internal (or contracted third-party) security engineers, penetration testing (PEN tests) identifies organizational weaknesses by simulating cyberattacks. They enable organizations to better understand and ultimately minimize risks.

Working with a partner, an organization typically starts by establishing a comprehensive map of its business functions, potential threats by function, and specific penetration testing goals by business area. The third-party then executes testing activities across a number of areas including: network, applications, systems, hosts and other critical computing resources.

Awareness Training: Awareness training is considered one the most effective mitigation techniques to combat cyberattacks. It is by far the best way to keep unsuspecting users from clicking on seemingly harmless links that lead to successful *Social Engineering* attacks.

A good security awareness program educates employees about corporate policies and procedures, but more importantly, it raises awareness by providing real-life examples of security threats. The National Institute of Standards and Technology NIST provides excellent guidelines and templates for ensuring the implementation of an effective employee awareness training program.

Administration: While many tools and techniques are available to secure the company's information assets, none is more critical than adopting a stringent security administration posture. Most cyberattacks result from a lack of adequate administration of critical resources.

Key areas of focus include:

- **Having the right security resource(s)** who are diligent at reading log files, analyzing reports and pursuing anomalies is crucial. A diligent security administrator can quickly highlight events that represent a potential threat while others fail to analyze anomalies that can result in a major risk.

- **Diligently patch systems, end-points and security appliances** to ensure the enterprise is not exposed to known threats. Updates and security patches are released on a regular basis to ensure up-to-date threat defense. Administrators should be diligent about ensuring patches are implemented on a timely basis.

- **Divide internal and third-party security administration policies and procedures.** By carefully dividing administrative responsibilities between internal engineers and MSSPs, the organization is provided with a system of checks and balances to ensure all parties are effectively managing the company's security fabric.

- **Proper administration of critical credentials and access methods is crucial**. The best source of information about how to orchestrate a cyberattack is often provided by system administrators. Often, administrators inadvertently leave sensitive notes to themselves in personal directories.

- An administrator’s home directory is often the first place an attacker examines once they have gained access. Security administrators should apply good housekeeping rules and regularly cleanup their directories to ensure sensitive privileged access information is removed or properly encrypted.

- **Clear security policies and procedures.** Security procedures and policies must be clearly outlined in writing and should specify what is acceptable behavior on networks, systems and computing resources. Users should be required to read and sign off on these procedures.

THE TAKEAWAYS

Protecting the organization against major cyberattacks can be overwhelming, not to mention expensive. It can be daunting to navigate through various solution strategies, partner and vendor offerings and services.

However, understanding the organization's security posture and capabilities is a critical first step to answer four key questions:

- What can I manage internally?
- What are the capabilities of my internal staff?
- What should I outsource to a third-party (and under what terms)?
- Which tools should I invest in?

By answering these four questions, an organization takes a critical first step towards establishing an overall cyber security strategy and defining who will carry responsibility (and accountability) for protecting the organization against cyberattacks.

AUTHOR

Anthony DeLima
CTO & Global Head of Digital Transformation
anthony.delima@neoris.com

ABOUT NEORIS
NEORIS is a leading global consultancy that unlocks business potential and drives Digital innovation to unleash significant industry disruption. NEORIS combines its industry knowledge and experience in disruptive technologies to create new interactive customer connections. The company leverages its knowledge of technology, people and design to create unique and innovative solutions that enable companies to deliver new business value to their customers. Headquartered in Miami, FL., NEORIS has a network of global delivery centers, design studios and operations in the U.S., Europe, Latin America, Africa, the Middle East and Asia.

www.neoris.com