Cybersecurity 101

Are you protected?

Are you protected?

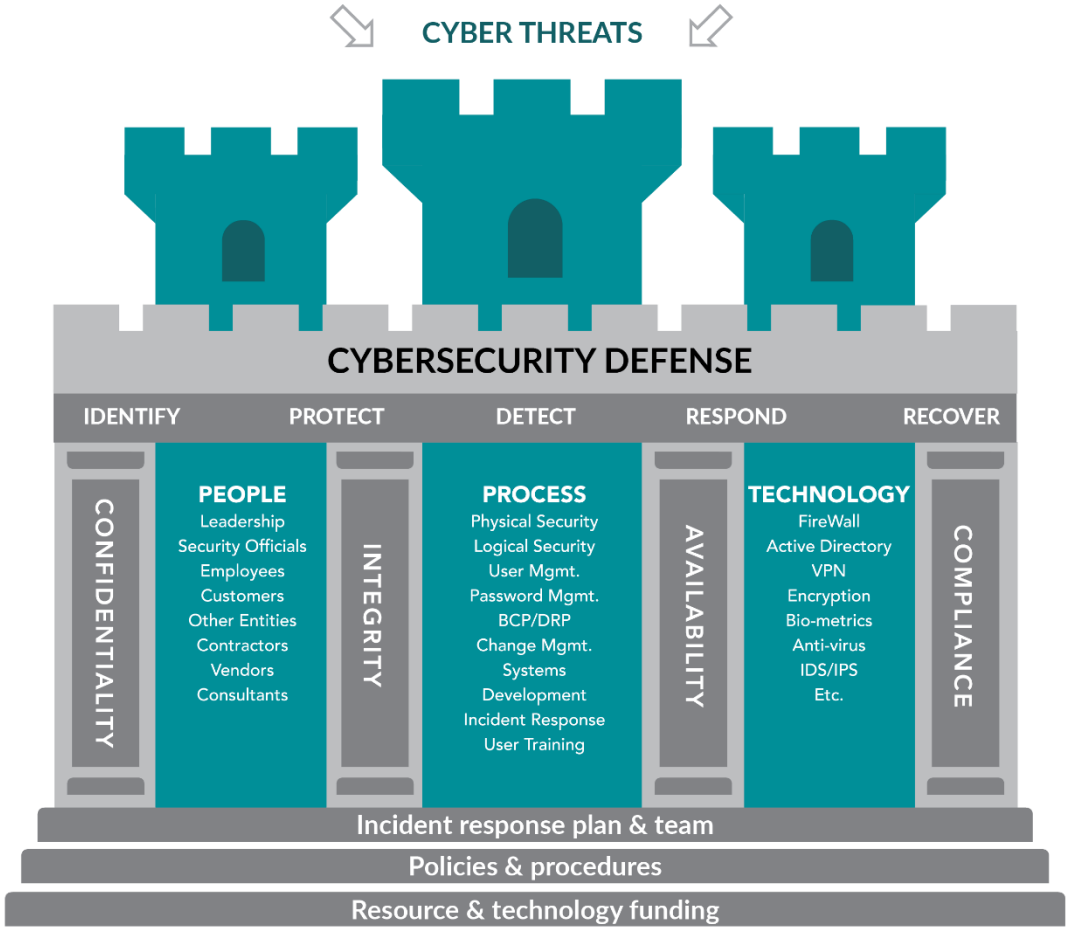
Have you considered?	Examples
Where is your sensitive, confidential data?	Payroll, credit card, intellectual property, financial, client, etc.
What are the consequences if that data was hacked?	Reputation, legal costs, forensic costs, etc.
Can your business continue to operate if IT systems are not available?	Loss of productivity
Are you meeting your security & privacy contractual & regulatory requirements?	HIPAA, GDPR, CCPA
What happens if your systems are locked by a hacker?	Ransomware
Do you have proper protections in place for social engineering threats like Phishing?	Malware, wire fraud
Who is responsible for cybersecurity and how much time do they spend on that effort weekly?	Skills, experience, etc.

Cybersecurity Program

Fortify your cybersecurity defenses with people, processes, and technology

Our cybersecurity experts can help you assess, test, and improve security to keep your technology investments protected and current.

Plante Moran has developed an overall framework that provides a comprehensive approach for developing an effective cybersecurity threat management program that utilizes a risk-based approach to map controls over the confidentiality, integrity, and availability of systems and data, as well as meet various security and privacy regulations.



Top 5 Cyber Threats

As cyberattacks grow more sophisticated, complex, and financially devastating, organizations still struggle to mitigate security breaches.

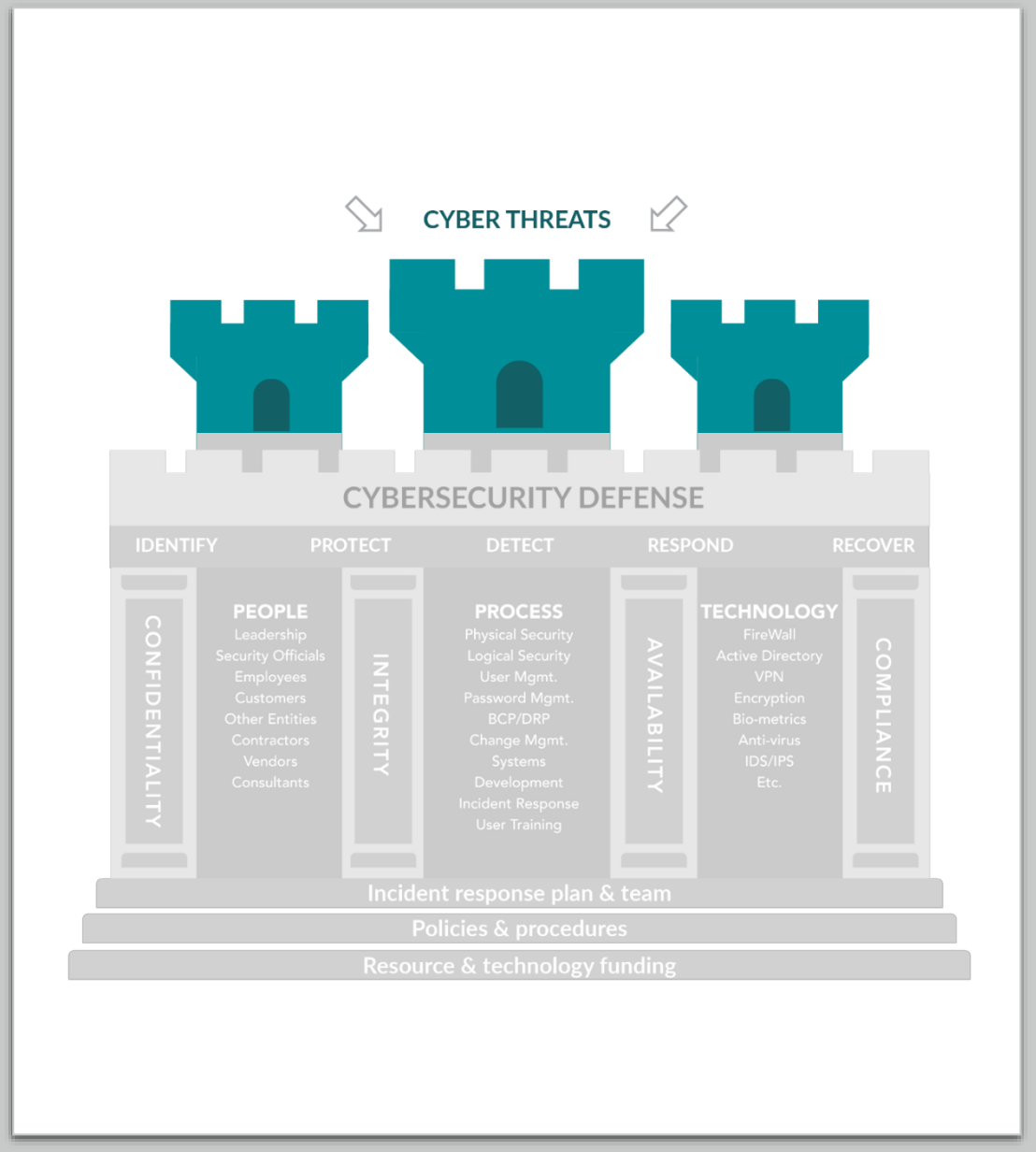
Phishing

Ransomware

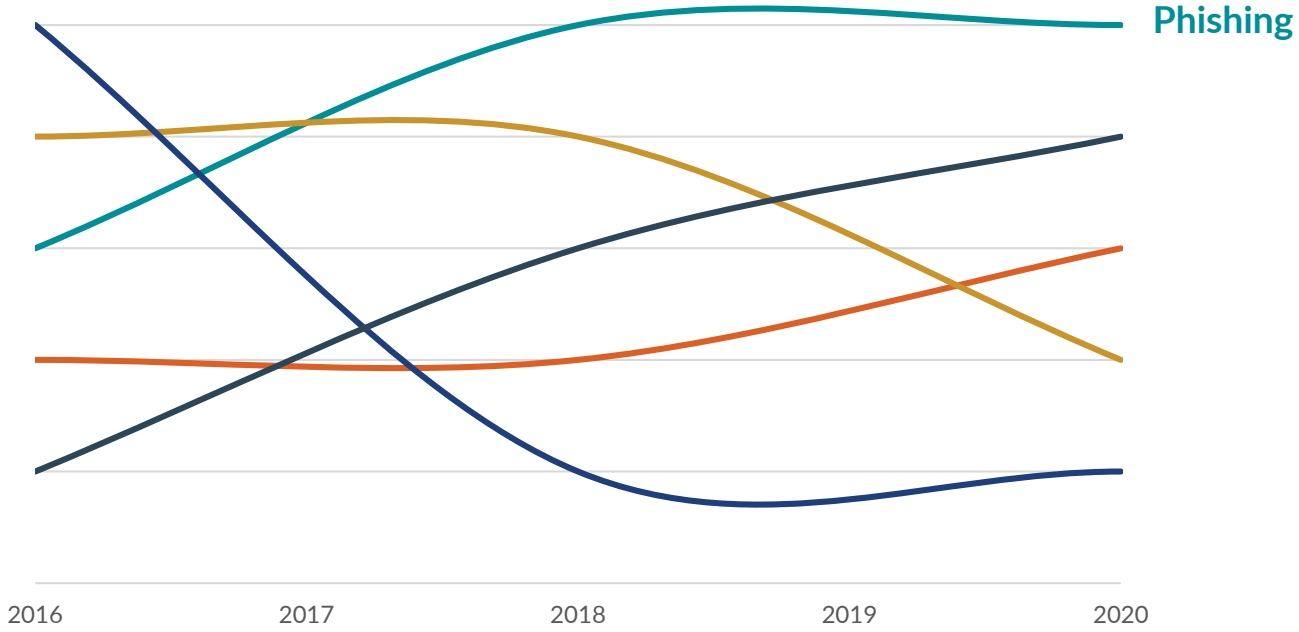
Malware

Password Compromise

Weak security configurations



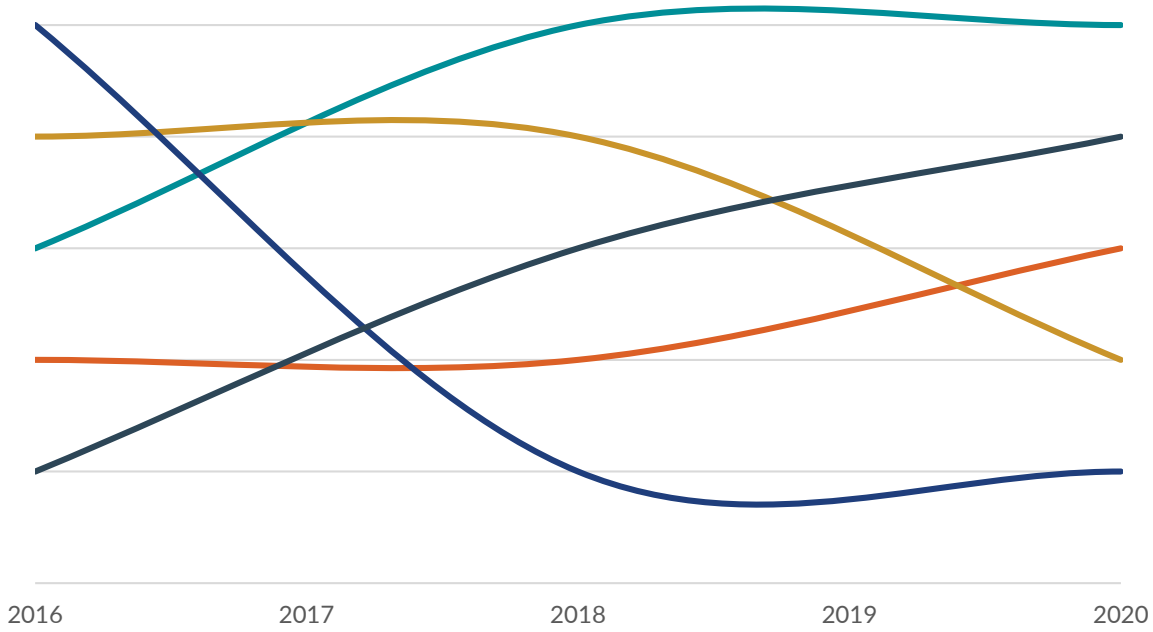
Cyber Threats



A fraudulent attempt to obtain sensitive data, such as passwords, credit card details, etc. by disguising oneself as a trustworthy entity in an electronic communication. Common impacts:

- Leads to further hacking using the compromised passwords
- Unauthorized wire-transfers or payments
- Unauthorized use of credit cards for online purchases.

Cyber Threats

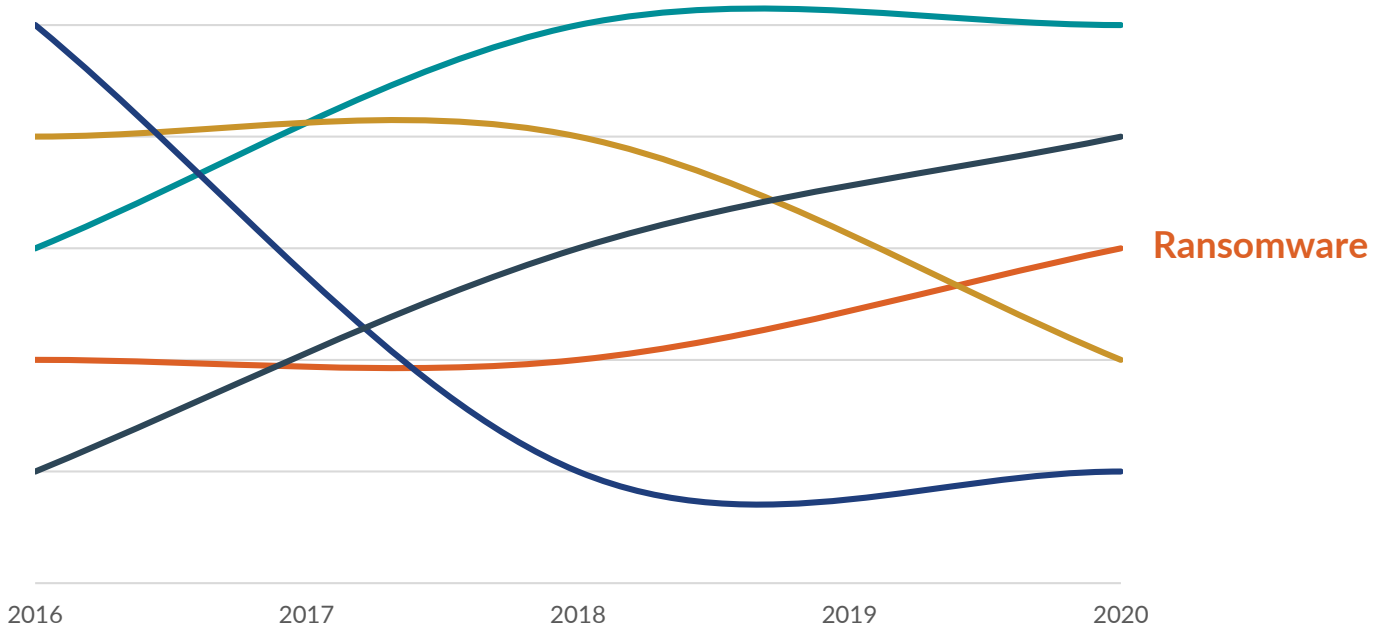


Weak Configuration

Weak network or cyber controls configuration allows hackers to exploit your network infrastructure. Often, companies aren't up to date on security patches leading to zero-day attacks. Common impacts:

- Common source of Ransomware attacks
- Loss of private or confidential data
- Backdoors for future attacks

Cyber Threats

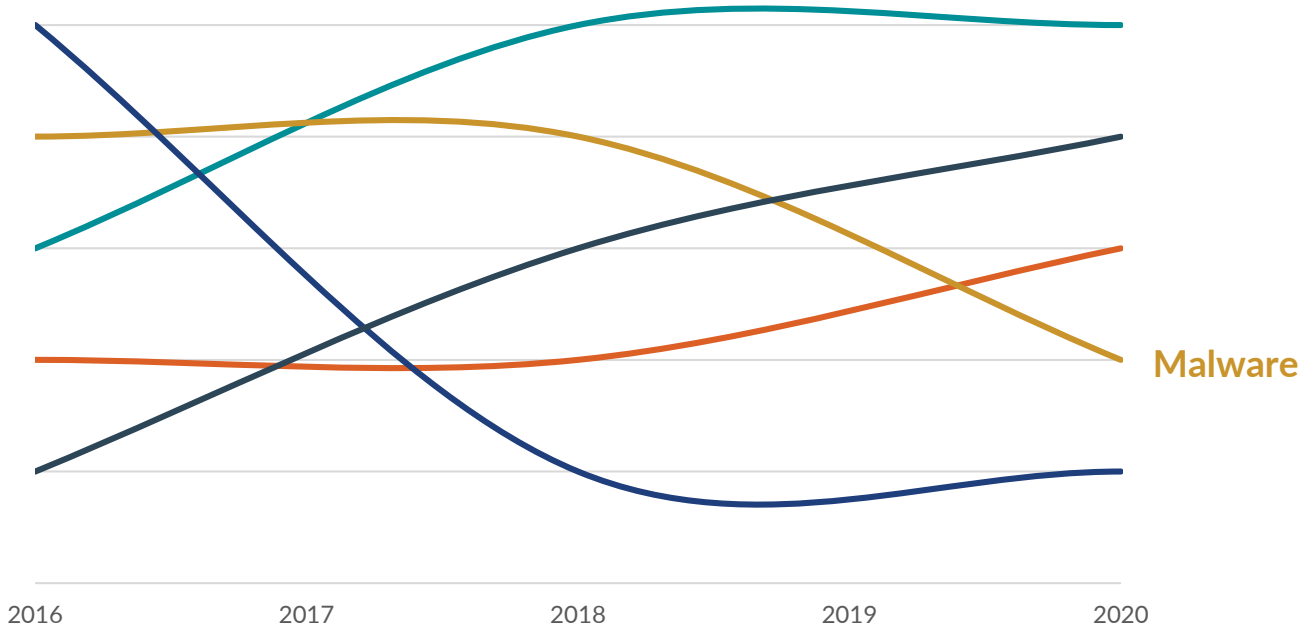


Hackers using malicious software that infects your IT systems by making them inoperable and demanding money to restore systems. Common impacts:

- Shut down of operations
- Dealing with hackers and finding proper methods to pay them
- Cyber insurance might not cover the payment

(Hackers may also hold companies at ransom by threatening to disclose private or confidential information on the internet – e.g. Sony Entertainment)

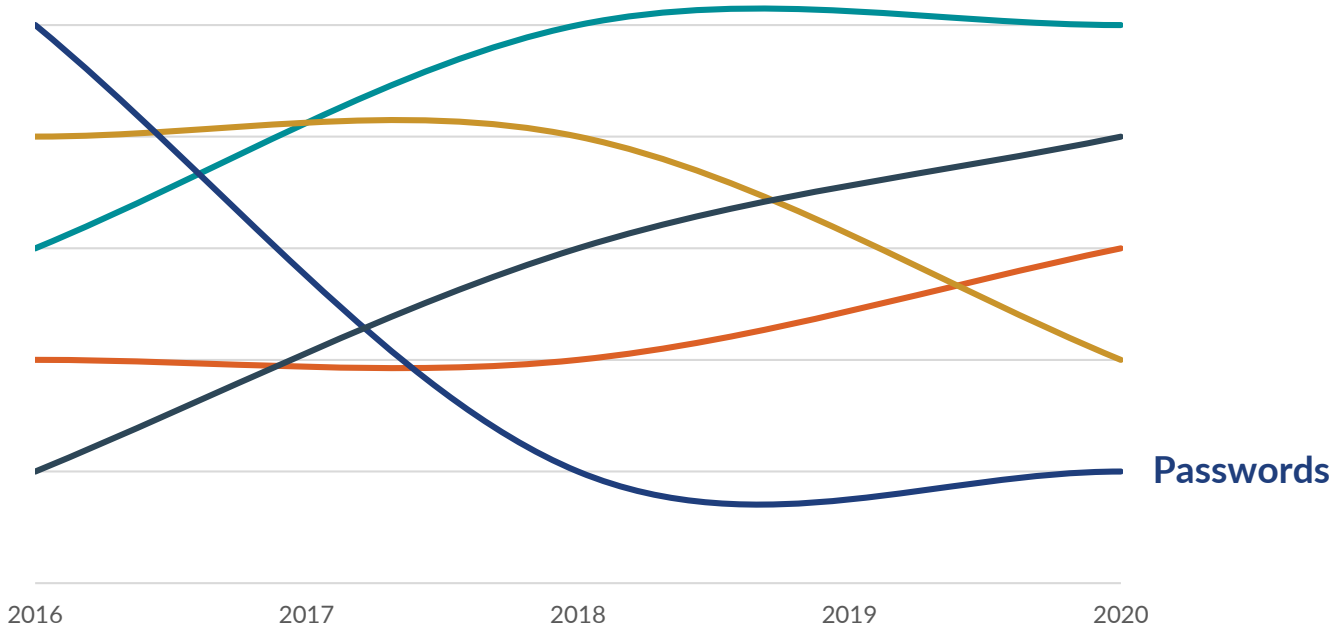
Cyber Threats



Software intentionally designed to cause damage to a computer system or network. Various types, including virus, worms, Trojan horses, spyware Common impacts:

- **Virus:** Software normally hidden within another software that can copy and insert into other programs or files. Normally causes harm by corrupting data.
- **Trojan Horse:** Software that misrepresents itself as a regular program or utility and carries a hidden destructive function.
- **Spyware:** software that gathers information about person or organization and send it to another entity.

Cyber Threats



Hackers exploit weak passwords by:

- Using a password cracking tool
- Guessing the password
- Use one stolen password for other sites

Other Cyber Threats

Organization

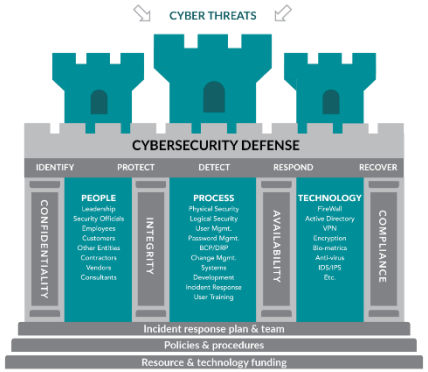
- Theft/loss of physical device
- Employee error/negligence
- Employee intentional fraud
- Accidental online disclosure
- Cyber attack at third-party
- Vulnerabilities in IoT devices
- Theft of intellectual property by departing employee

COVID

- Remote workers
- Increased use of laptops and personal devices
- Weak security on home networks
- Increased opportunities
- Desperate criminal hackers

Technology Trends

- Increased use of Cloud
- Integration of IoT devices



Cyber attacks in August 2020

VPN Passwords Leaked

Alexa Speech History Exposed

Jack Daniels Targeted

Cyber attacks

- **15-year-old Merseyside boy arrested for hacking UK PayPal account** (unknown)
- **Leeds-based Luminate Education Group hit by cyber attack** (unknown)
- **Myerscough College hit by cyber attack on exam results day** (unknown)
- Mexican delivery startup iVoy experiences data breach (127,432)
- Cyber attack affects website of Texas-based Hudson Independent School District (unknown)
- Hacker leaks passwords for enterprise VPN servers (913)
- Intel investigating breach after 20GB of internal documents leak online (unknown)
- FX broker Pepperstone has updates its clients over third-party malware attack (unknown)
- Scholarship America notifies individuals of breach (unknown)
- Indiana-based Community School Corporation of Southern Hancock County hit by cyber attack (unknown)
- Ohio-based Premier Health Partners discloses data breach (unknown)
- The SANS cybersecurity training organisation hit by phishing scam (unknown)
- Pakistani intelligence agencies have tracked a major security breach by Indian hackers (1,400)
- North Korean hacking group attacks Israeli defence industry (unknown)
- Canada Revenue Agency records breached in a pair of cyber attacks (5,500)
- Germany's military-run transport fleet hacked (unknown)
- Rochester City School District reopening forum hacked on Zoom (unknown)
- Experian SA incident affects millions of South Africans (24 million)
- Incident at Louisiana's Jefferson Parish public school affects students (86)
- Mitsukoshi and MI Card confirm that its systems were hacked (19,000)
- Kariyer.net customers hit by security incident (55,149)
- Hacker breaks into royalty-free photo site Freepik (8.3 million)
- CO-based Mental Health Partners says an employee's account was hacked (unknown)
- Sumitomo Forestry Co., Hitachi Chemical Co. among Japanese firms affected by VPN vulnerability (unknown)
- CA-based North Okanagan Pediatric Clinic informs patients of cyber attack (unknown)
- New Zealand stock exchange disrupted by fourth 'offshore' cyber attack (unknown)
- Nevada's Clark County School District provides few details of security incident (unknown)
- Utah Pathology Services notifying patients of security incident (112,000)

Data breaches

- **Basingstoke Hospital investigating possible confidentiality breach** (unknown)
- **Password displayed in Plymouth government building window**(unknown)
- **Passer-by finds sensitive medical info belonging to Caithness General Hospital** (19)
- **Southern Water customers could view others' personal data by tweaking URL parameters**(unknown)
- Robocall legal advocate Blacklist Alliance leaks customer data (388)
- Twitter says security flaw may have exposed Android users' direct messages (unknown)
- Canadian transport firm Metrolinx investigating privacy breach (2,000)
- MedEvolve finally discloses security incident two years after it occurred (unknown)
- Argentinian government exposes COVID-19 health data (115,000)
- Ireland's Department of Employment Affairs and Social Protection leaks sensitive data (unknown)
- Researchers uncovered Alexa flaw that exposed personal information and speech histories (unknown)
- BioTel Heart leaves cardiac patient data exposed online (61,000)
- Hacker releases the databases of Utah-based gun exchanges (281,999)
- Researcher discovers Github databases from nine US medical entities (150,000)
- New South Wales Police force leaks emails relating to Black Liver Matter protest (150)
- Co Cork's Union Quay Medical Centre sent STD and mental health diagnoses to the wrong patient (2)
- AI company Cense leaked information from car accident victims (2.41 million)
- Canada's London Police Service snooped on records of people who tested positive for COVID-19 (10,475)
- Managed isolation facility security guard suspended over social media privacy breach (27)
- Records from West Texas Orthopedics found in recycling centre (unknown)
- South African social grant applications were found dumped on the street (unknown)
- India's most popular travel booking hubs was left exposed (700,000)
- Wellington-Dufferin-Guelph Public Health notifies those affected by data breach (unknown)
- New South Wales driver's licences found in open Cloud storage (54,000)
- Manitoba government confirms privacy breach at Children's Disability Services (9,000)
- Philadelphia Archdiocese clergy abuse victims part of accidental email leak (47)

Ransomware

- **British Dental Association records leaked on the dark web** (5,524)
- Australian aged care firm Regis hit by ransomware (unknown)
- Canon suffers ransomware attack that impacts numerous services (unknown)
- Lafayette, CO, gov pays $45,000 in ransom after computer systems were disabled (unknown)
- Coronavirus ventilator manufacturer Boyce Technologies targeted by ransomware gang (unknown)
- Three US medical practices hit by ransomware (unknown)
- Multiple systems impacted by ransomware attack on California-based Imperial Valley College (unknown)
- Jack Daniel's manufacturer target of apparent ransomware attack (unknown)
- Medical debt collection firm R1 RCM hit in ransomware attack (unknown)
- OK-based Ponca City Schools had backups to prevent ransomware disaster (unknown)
- Baugo Community Schools in Indiana dealing with cyber attacks (unknown)
- Canadian land developer Brookfield Residential hit with ransomware (unknown)
- Delivery firm Canpar Express faces delays amid ransomware attack (unknown)
- NC's Haywood County schools shut down by ransomware (unknown)
- No ransomware paid after Ventura Orthopedics hit by ransomware (1,850)
- Arkansas' Gosnell School District is recovering from a ransomware attack (unknown)
- CA-based Rialto Unified suspends online learning amid ransomware (unknown)
- Valley Health System recovering from ransomware attack while maintaining patient care (unknown)
- California's Selma Unified School District hit by ransomware (unknown)
- North Carolina's Greenville Technical College suffers ransomware attack (15,000)
- Houston's United Memorial Medical Center hit by ransomware (unknown)
- Rocky Mount, North Caroline, hit by ransomware (unknown)
- Amphastar Pharmaceuticals learns that hackers exfiltrated employee data in ransomware attack (unknown)
- Cruise ship operator Carnival crippled by ransomware (unknown)

Malicious insiders and miscellaneous incidents

- Nova Scotia Health notifying patients affected by two separate incidents (211)
- Arkansas-based Ashley County Medical Center fires nurse for improperly accessing patient records (722)
- Iran cover-up of deaths revealed by data leak (200,000)
- Former employee at NC-based Coastal Preparatory Academy stole sensitive data (unknown)
- Rogue employee to blame for breach at Turkey's Rezzan Günday (unknown)
- Employee at IL-based Villa at Palos Heights paid bills with patients' info (unknown)
- Cisco engineer resigns then nukes WebEx accounts (16,000)

Approach to combat cyber threats

To keep hackers from exploiting all-too-common vulnerabilities, it takes a strong and coordinated defense that includes three major controls: people, process, and technology.

People

End users are your first line of defense from attacks. With the best intentions to provide fast service, employees may click on links or attachments in phishing emails in an effort to fulfill seemingly legitimate requests. But doing so enables hackers — unbeknownst to you — to install malicious software, request credentials such as passwords and security questions and answers, and initiate wire transfers.

Process

As threats constantly evolve, your processes to detect and resolve new threats must evolve as well. Patches to operating systems and third-party applications, for example, must be rigorously maintained to protect against the latest vulnerabilities. Your recovery planning process, too, needs to evolve to adequately address the increased new threats, such as ransomware.

Technology

While IT supports and facilitates your operations, it also must secure sensitive data and information entrusted to your organization. Strong controls are critical, whether you manage your IT organization in-house or outsource. You must ensure, not assume, vendor processes and controls align with the latest security protocols and your organization's and stakeholders' expectations.

Cybersecurity Services

While we provide a complete range of planning, value-added, risk mitigation, and compliance services, these are the top focus areas.

7-Point cybersecurity assessment

Our 7-point cybersecurity assessments focus on major security concerns and effective controls throughout the organization to determine the IT security posture and identify vulnerable areas.

Attack & pen testing

Using the most current threat intelligence, our cybersecurity specialists work with you to identify specific target areas and launch controlled cyber attacks from common footholds to identify gaps and weaknesses.

Security awareness training

Our team delivers training content based on state-of-the-art best practices and your organization's distinct environment, needs, and concerns.

Social Engineering

Since phishing messages targeting employees are commonly an attacker's initial foothold into your environment, our team works with you to develop a phishing email campaign and track responses to identify staff awareness training opportunities.

Incident response tabletop exercise

The tabletop exercise will help assess the effectiveness of your organization's ability to recover from a cyber incident. The exercise not only looks at the written plan but also the process, tools and technologies, and team involved in the recovery efforts.

Scott Petree, Principal
scott.petree@plantemoran.com
p. 248.223.3898 | c. 734.546.6899

Thank you!