2024 WISCONSIN COUNTIES ASSOCIATION
LEGISLATIVE CONFERENCE

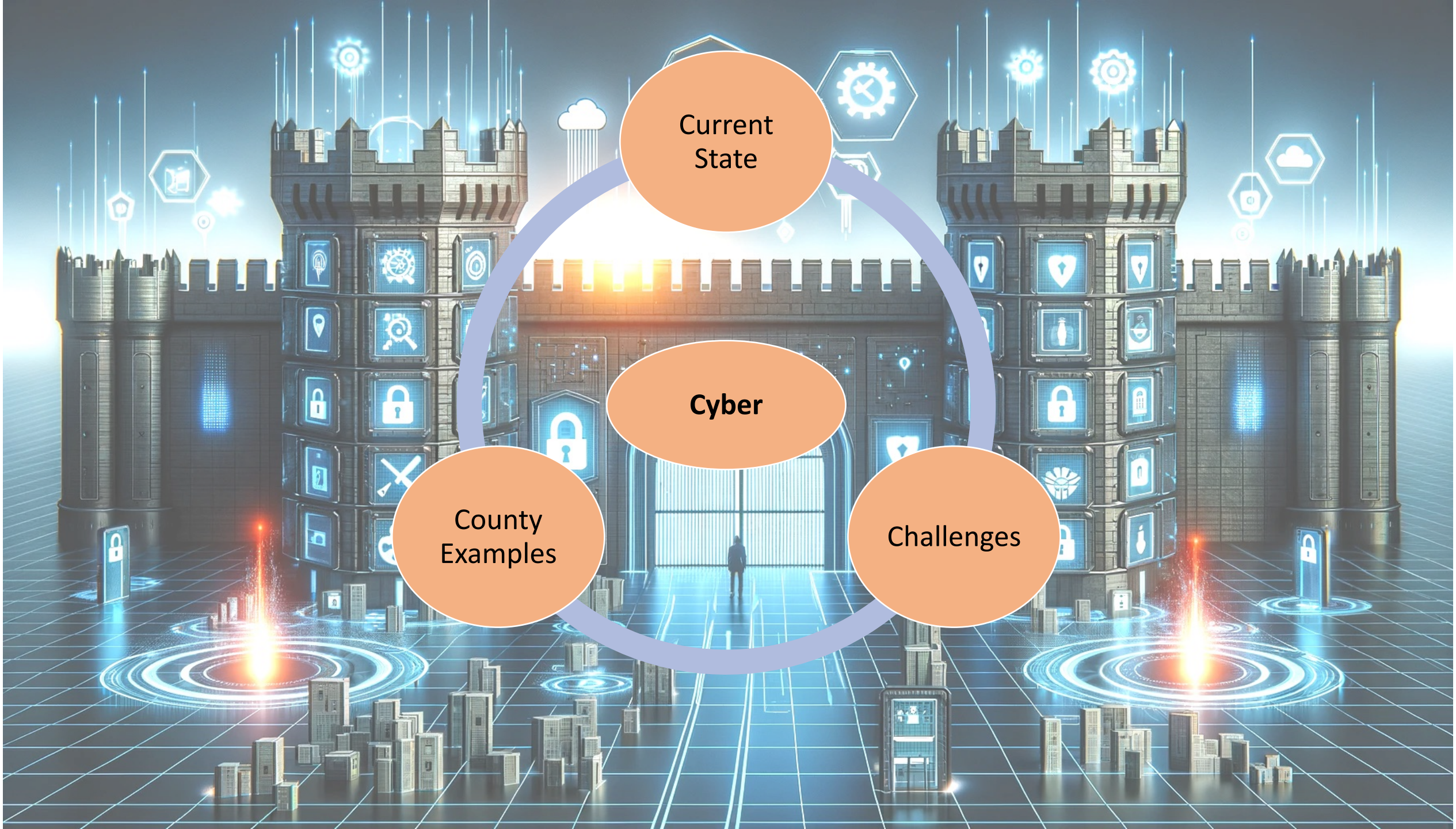
NATIONAL ASSOCIATION of COUNTIES NACo

How to Minimize Cyber Attacks on the County Castle

Rita Reynolds, NACo CIO

Rick McMillin, IT Operations Manager, Waukesha County

Tim Rahschulte, Executive Vice President, PDA


Current State
Cyber
County Examples
Challenges

By **CHRIS RIOTTA** // AUGUST 3, 2023

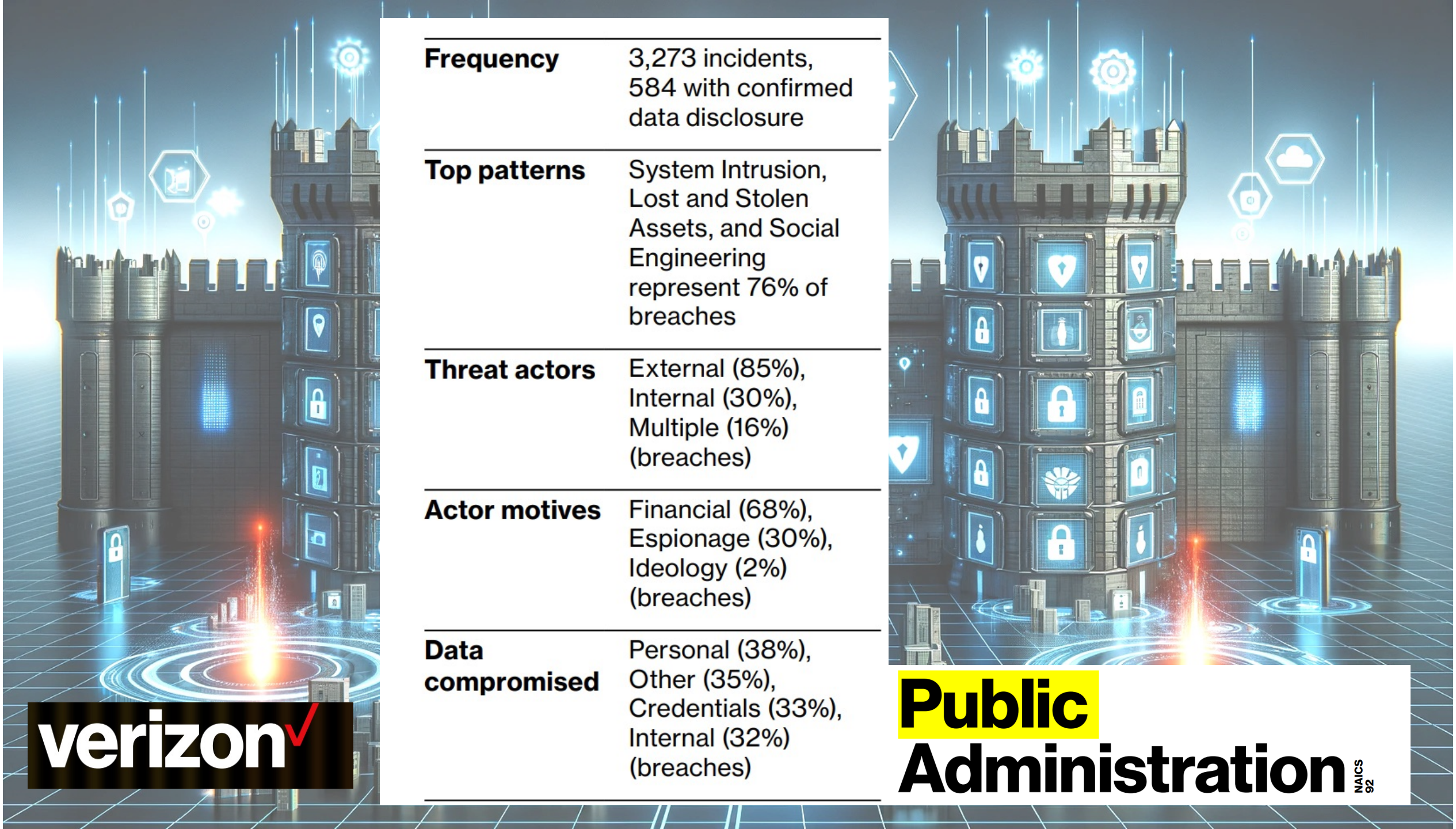
NEXTGOV/FCW

Cyberattacks impacting government agencies and the public sector spiked by 40% in recent months, according to a new report.

Current Statistics and News

Research has shown that government agencies and law practices experienced the largest spike i ransomware attacks at 95% in quarter three of 2023. Moreover, global ransomware attacks were up by 95% in the third quarter of 2023 when compared to the same period in 2022.

IT SECURITY GURU



verizon✓

Frequency	3,273 incidents, 584 with confirmed data disclosure
Top patterns	System Intrusion, Lost and Stolen Assets, and Social Engineering represent 76% of breaches
Threat actors	External (85%), Internal (30%), Multiple (16%) (breaches)
Actor motives	Financial (68%), Espionage (30%), Ideology (2%) (breaches)
Data compromised	Personal (38%), Other (35%), Credentials (33%), Internal (32%) (breaches)

Public Administration

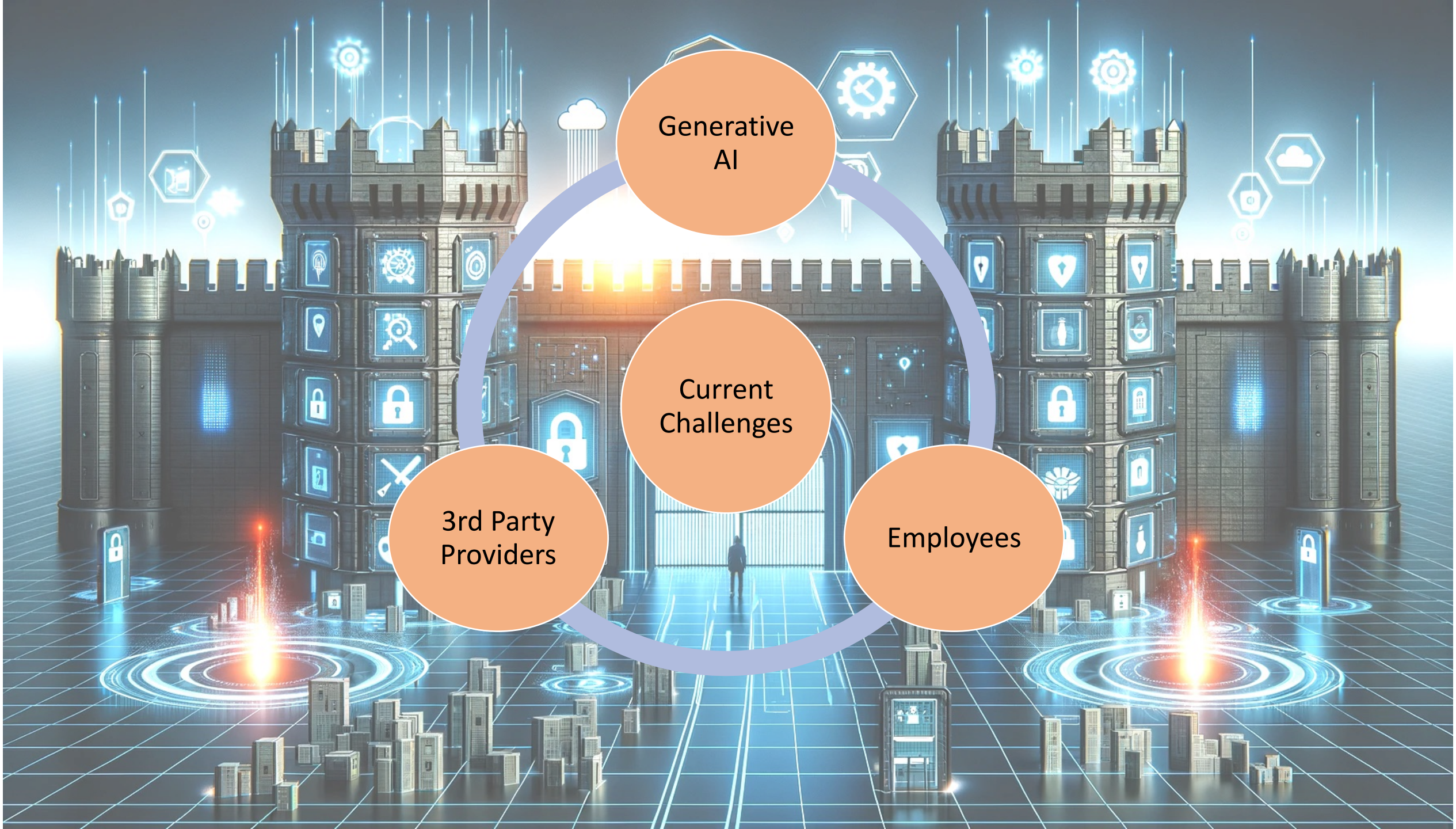
NAICS 92

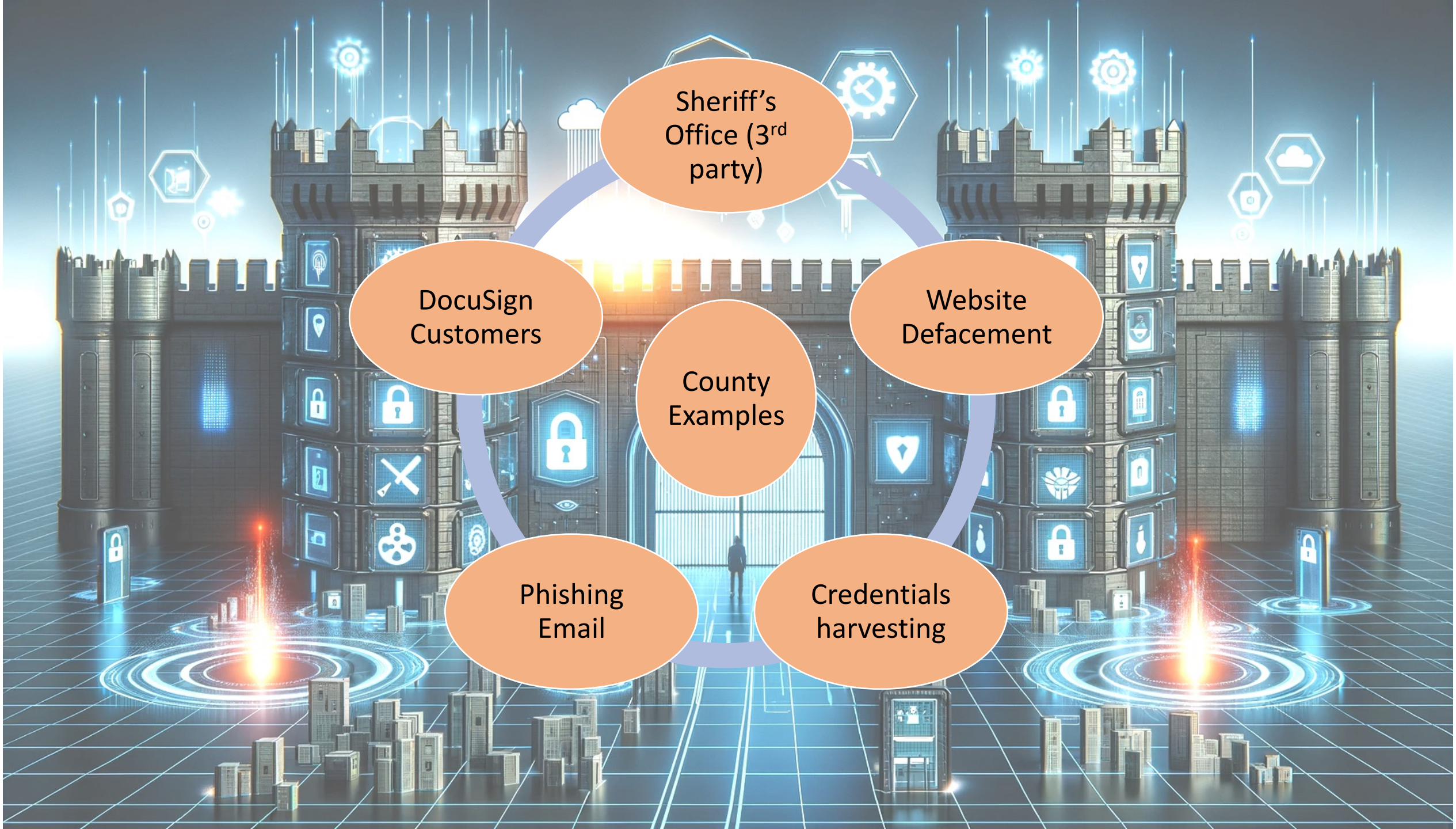
By Blayne Alexander and Zoë Richards

NBC NEWS

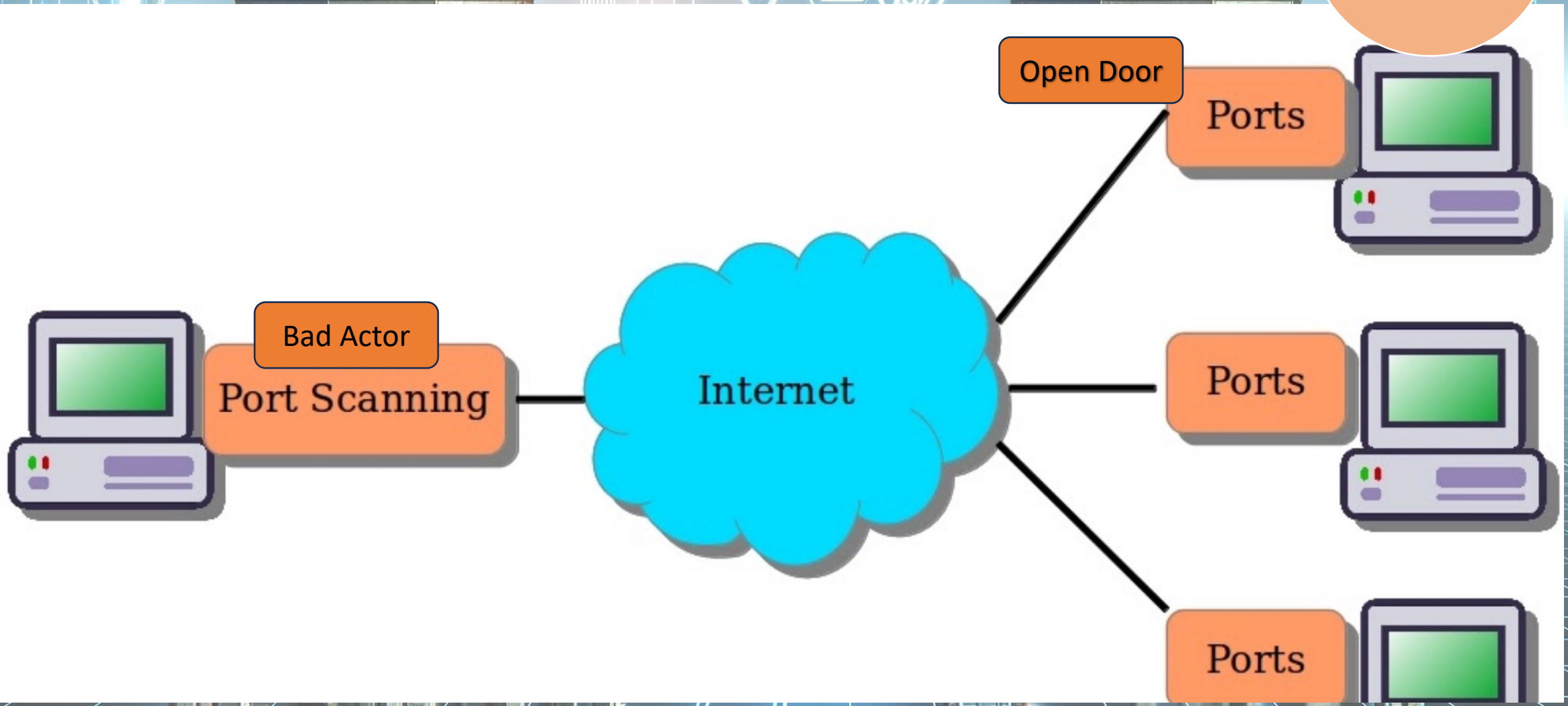
ATLANTA — A cyberattack that hit government systems in Fulton County, Georgia, over the weekend affected the offices of the district attorney who is prosecuting former President Donald Trump on election interference charges, local officials said Monday.

All desktop phones, intranet and devices using county servers are down for all departments, including District Attorney Fani Willis' office, said a county official with knowledge of the situation.

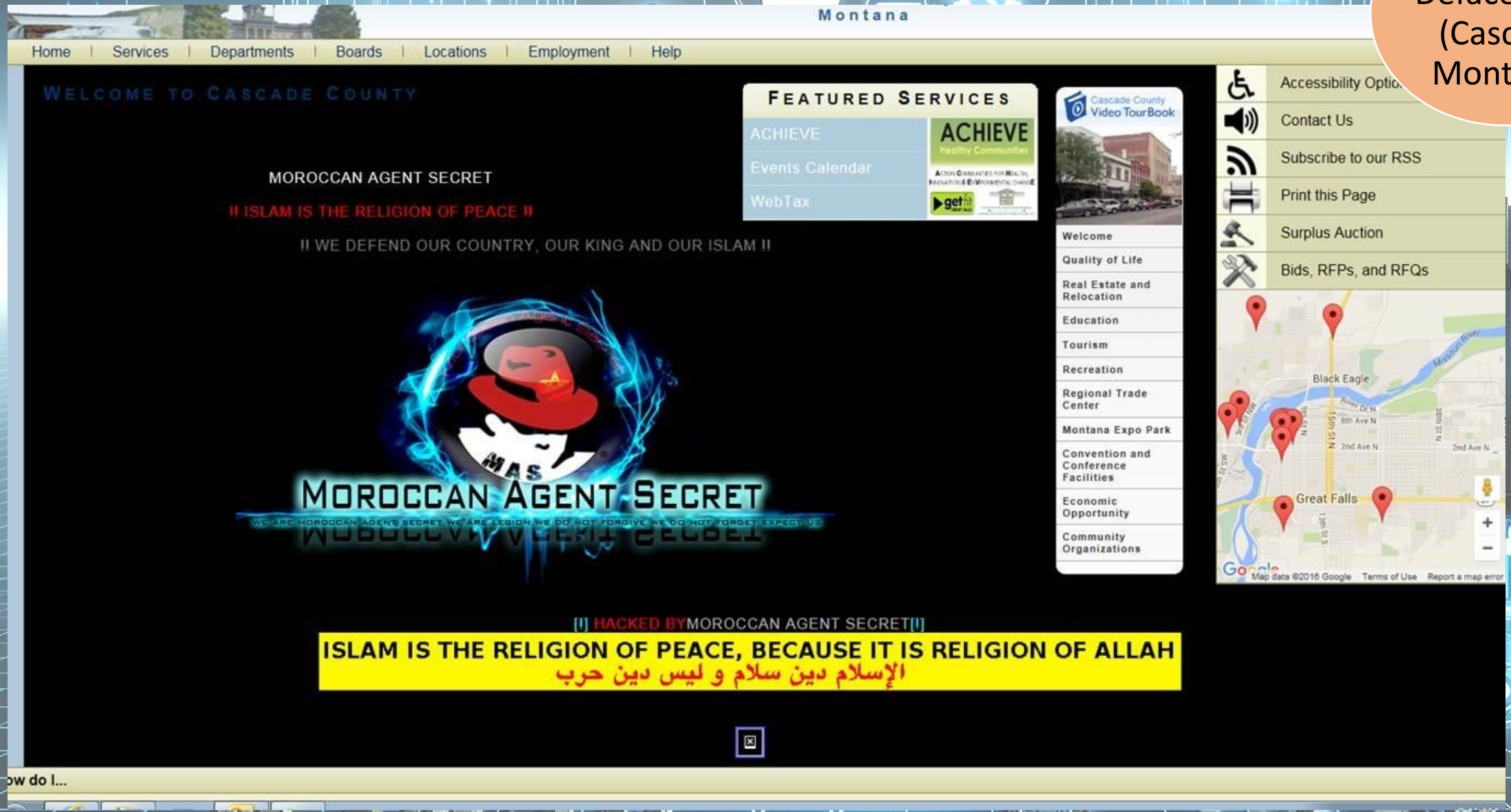

Generative AI
Current Challenges
3rd Party Providers
Employees

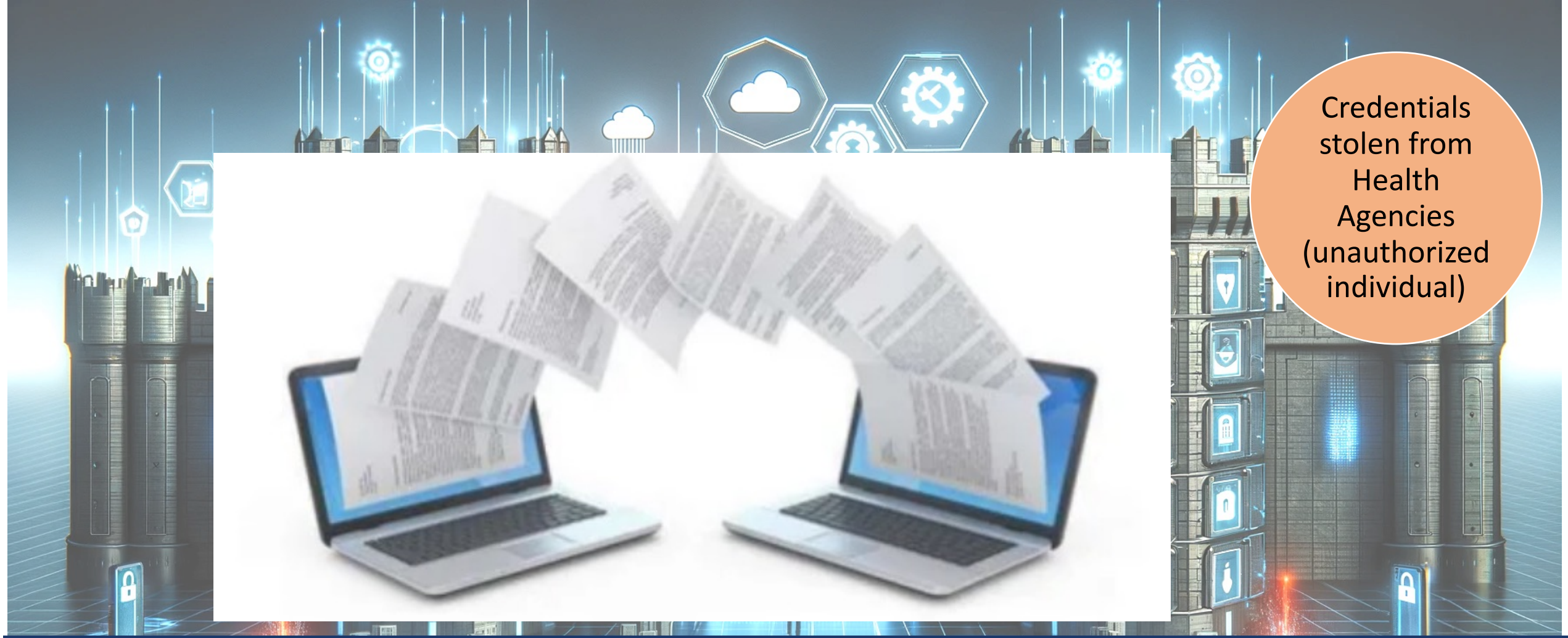

Sheriff's Office (3rd party)
DocuSign Customers
Website Defacement
County Examples
Phishing Email
Credentials harvesting

Sheriff's Office (3rd party)



Website Defacement (Cascade Montana)





Credentials stolen from Health Agencies (unauthorized individual)

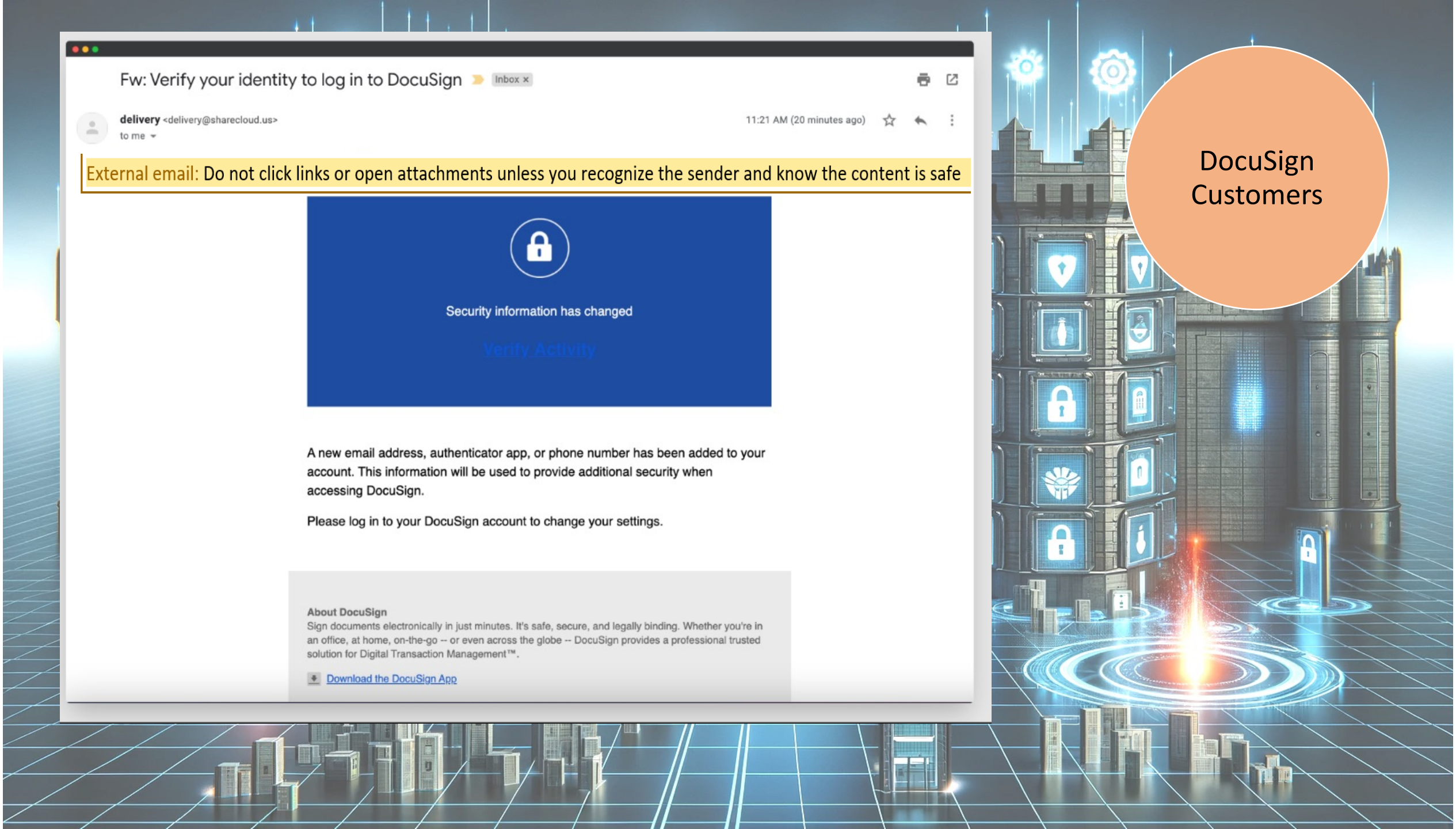
NBC 5 CHICAGO LOCAL WEATHER VIDEO INVESTIGATIONS ENTERTAINMENT SPORTS ...

Cook County Health data breach exposes personal information of 1.2M patients

Phishing Email - Dallas

DALLAS (CBSNewsTexas.com) — An international cyber hacker group is threatening to publish sensitive information it claims it stole from the Dallas County computer system unless the county pays a ransom by Friday.

County officials confirmed a cyber incident was detected on Oct. 19. The county hired outside cybersecurity experts to help contain it and officials said it prevented any files from being encrypted.


Fw: Verify your identity to log in to DocuSign
Inbox ×
delivery <delivery@sharecloud.us>
to me
11:21 AM (20 minutes ago)
External email: Do not click links or open attachments unless you recognize the sender and know the content is safe
Security information has changed
Verify Activity
A new email address, authenticator app, or phone number has been added to your account. This information will be used to provide additional security when accessing DocuSign.
Please log in to your DocuSign account to change your settings.
About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.
Download the DocuSign App
DocuSign Customers

POST ONLINE MEDIA

Bucks County, Pennsylvania emergency dispatch system down for days due to cyberattack

READING TIME 1 MIN CHRISTIAN FERNSBY ▾ | January 28, 2024

Law enforcement officials in Bucks County, Pennsylvania are working to restore services to its computer aided dispatch system, or CAD system, after a cyberattack crippled the service.

Fulton County government outage: Cyberattack brings down phones, court site and tax systems

By Alta Spells, Devon Sayers, Jason Morris and Sean Lyngaas, CNN

3 minute read · Updated 12:33 PM EST, Tue January 30, 2024

Exterior view of the Fulton County Courthouse. Kevin Dietsch/Getty Images/File

Waukesha County Cyber Attack

November 3, 2023

Save As | Save All Attachments | Upload | Upload All Attachments | Show Message | ...

FW: Doc Copy Invoice#60181 CRM:69001

GC

Gabriel Christenson <GChristenson@hebronhouse.org>
To Gabriel Christenson

Reply | Reply All | Forward | ...

Fri 11/3/2023 11:42 AM

Doc Copy Invoice#60181 CRM:69001 (8.17 KB)
Outlook item

CAUTION: This email originated from an unverified external source. Verify the legitimacy of the email before clicking links or opening attachments. If you believe this email is malicious in nature, please report it by using the Phish Alert button in Outlook.

Please see attached.

Thanks
Gabriel

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acce...	Authentication re...
11/3/2023, 3:01:22 PM	e8d03086-f8e2-4a36-...	[redacted]	Netsmart NIAM PROD	Success	205.213.17.9	Waukesha, Wisconsin,...	Success	Single-factor authenti...
11/3/2023, 12:24:38 PM	a3737162-b43b-4ffa-...		OfficeHome	Failure	88.216.214.215	Chicago, Illinois, US	Failure	Multifactor authentic...
11/3/2023, 12:23:24 PM	866e9cb6-a1fd-4f99-...		OfficeHome	Interrupted	154.7.255.39	Sheridan, Wyoming, US	Failure	Multifactor authentic...
11/3/2023, 12:23:13 PM	5aa6d4f5-b531-488a-...		OfficeHome	Failure	45.58.228.227	Waterloo, Ontario, CA	Failure	Multifactor authentic...
11/3/2023, 12:13:24 PM	d8448d4f-861e-4988...		Netsmart NIAM PROD	Success	205.213.17.9	Waukesha, Wisconsin,...	Success	Single-factor authenti...
11/3/2023, 12:10:29 PM	99b6c4eb-8ca0-4075...		Microsoft Account Co...	Success	205.213.17.9	Waukesha, Wisconsin,...	Success	Single-factor authenti...
11/3/2023, 12:10:28 PM	59499eec-a3b6-474d...		Microsoft 365 Suppor...	Success	205.213.17.9	Waukesha, Wisconsin,...	Success	Single-factor authenti...
11/3/2023, 12:09:59 PM	10e062a2-4392-43e5...		OfficeHome	Interrupted	23.155.136.33	Santa Fe, New Mexico...	Failure	Multifactor authentic...
11/3/2023, 11:58:10 A...	63726bfe-a371-4219-...		OfficeHome	Interrupted	154.64.225.97	New York, New York, ...	Failure	Multifactor authentic...
11/3/2023, 11:52:14 A...	e5165cc9-28a1-4f9f-...		OfficeHome	Interrupted	104.36.84.103	Ashburn, Virginia, US	Failure	Multifactor authentic...
11/3/2023, 11:52:05 A...	1cfe30cf-a47a-4e63-...		OfficeHome	Interrupted	45.135.163.24	Lima, Ohio, US	Failure	Multifactor authentic...
11/3/2023, 11:47:28 A...	0ae7b4c0-10c9-42f9-...		OfficeHome	Failure	154.9.249.186	Hoboken, New Jersey,...	Failure	Multifactor authentic...
11/3/2023, 11:44:28 A...	9f54f426-819b-4fa0-...		Windows Sign In	Success	205.213.17.9	Waukesha, Wisconsin,...	Not Applied	Single-factor authenti...

Take Aways

- MFA
- Cyber Assessments
- Monitoring (MS-ISAC)
- CISA Resources
- Preparedness
  - Security Policy
  - Practice Sessions
  - Cyber Simulations
  - Build Relationships

Quick Question

Name the most effective, and most vulnerable, perimeter defense mechanism securing your data assets today?

HINT

There is a single word ‘right’ answer to this question.

CYBERSECURITY IS A TEAM SPORT

PEOPLE

are the most effective, and most vulnerable, perimeter defense mechanism securing your data assets today.

People are the perimeter.

CYBERSECURITY IS A TEAM SPORT

PEOPLE are the perimeter and COLLABORATION is the key

Understand the changing landscape of cyber threats

Assess and grow your team's cyber readiness

Document your plans for defense and recovery

CYBERSECURITY IS A TEAM SPORT

PEOPLE are the perimeter and COLLABORATION is the key

CISA CYBER+INFRASTRUCTURE

cisa.gov

NATIONAL ASSOCIATION of COUNTIES NACo

naco.org

WCA WISCONSIN COUNTIES ASSOCIATION

wicounties.org

Prepare for, respond to, and mitigate the impact of cyberattacks.

CISA
CYBER+INFRASTRUCTURE

CYBER ESSENTIALS

Your success depends on ***Cyber Readiness***. Both depend on ***YOU***.

THE LEADER'S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:

- YOUR ABILITY TO OPERATE / ACCESS INFO
- YOUR REPUTATION / CUSTOMER TRUST
- YOUR BOTTOM LINE
- YOUR ORGANIZATION'S SURVIVAL

Managing cyber risks requires building a culture of cyber readiness.

Essential Elements of a *Culture of Cyber Readiness*:

Yourself *- The Leader*

Drive cybersecurity strategy, investment and culture

Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money.

Your investment drives actions and activities that build and sustain a culture of cybersecurity.

Your Staff *- The Users*

Develop security awareness and vigilance

Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.

Your Systems *- What Makes You Operational*

Protect critical assets and applications

Information is the life-blood of any business; it is often the most valuable of a business' intangible assets.

Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

Your Surroundings *- The Digital Workplace*

Ensure only those who belong on your digital workplace have access

The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do.

Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

Your Data *- What the Business is Built On*

Make backups and avoid the loss of information critical to operations

Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted.

Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

Your Actions Under Stress

Limit damage and quicken restoration of normal operations

The strategy for responding to and recovering from compromise: plan, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans.

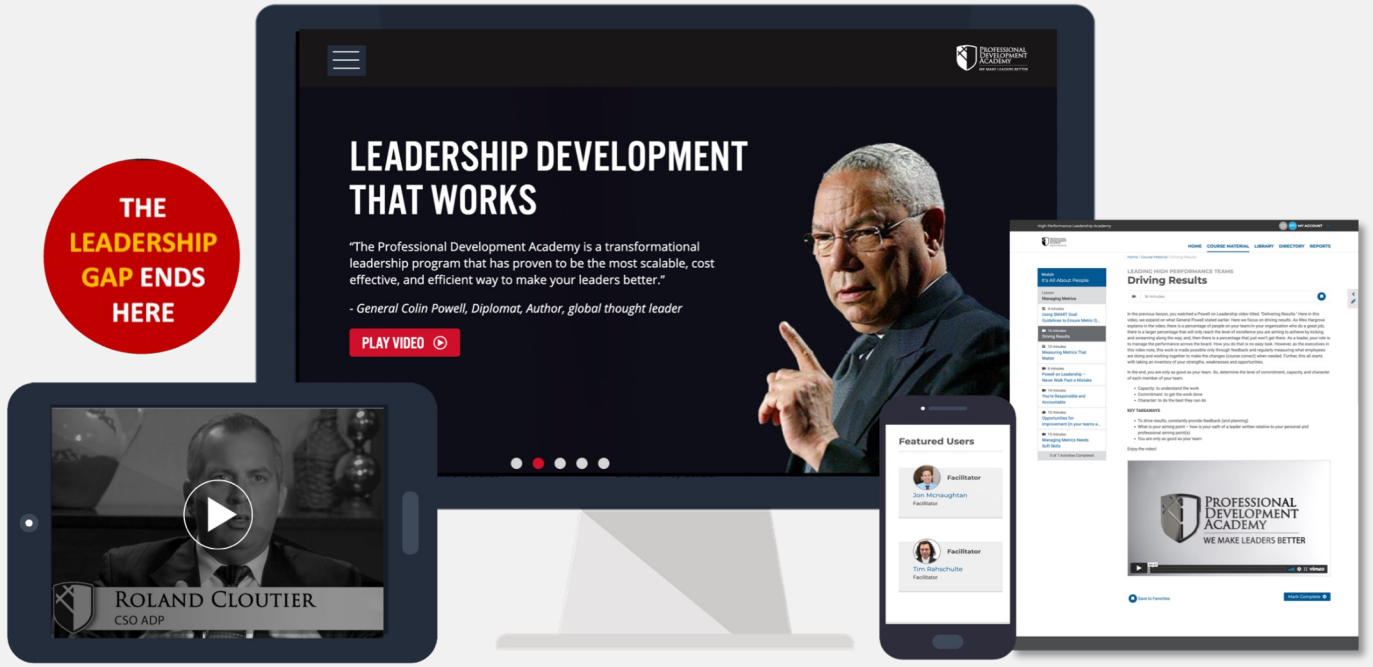
This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.

CISA.gov/Cyber-Essentials

For tech specs on building a Culture of Cyber Readiness, flip page ▸

The NACo Cybersecurity Leadership Academy

The Cybersecurity Leadership Academy enables the exchange of best practices and insights to support the growth and success of current government leaders and help emerging leaders prepare to address the myriad of challenges facing them today and in the future.



Two types of programs to choose from.

CYBERATTACK SIMULATION

weeklong reality-based, certified assessment that focuses on helping leaders of government organizations better protect and maintain their critical assets

CYBER LEADER ACADEMY

12-week online training facilitated to make existing leaders better and emerging leaders ready to address the most pressing cyber issues of today

The NACo Cybersecurity Leadership Academy

FREE

www.naco.org/cyberskills

timr@pdaleadership.com

SCHOLARSHIPS AVAILABLE

Two types of programs to choose from.

CYBERATTACK SIMULATION

weeklong reality-based, certified assessment that focuses on helping leaders of government organizations better protect and maintain their critical assets

CYBER LEADER ACADEMY

12-week online training facilitated to make existing leaders better and emerging leaders ready to address the most pressing cyber issues of today

Start with a conversation,
then commit, then continue.

Start with a conversation, then commit, then continue.

1. **Full system inventory:** A list of all assets and devices, including APIs, software programs, and other tools (local and in the cloud) is available and regularly updated.
2. **Backup and recovery system:** All systems and data are cataloged and ranked as critical priority 1-2-3, and a full back up system is in place and tested (along with recovery time) regularly.
3. **Segmented network access:** Critical data are segmented (separated) from single points of access so that if or when a breach occurs the data that are accessed is limited.
4. **Detection systems:** In addition to traditional firewalls, ransomware protection software and (early) detection system protocols are in place and tested regularly.
5. **Trained workforce:** Regular security awareness training (pre-scheduled and "surprise" attacks) is mandatory and integrated into the business culture with a mindset of "see something, say something."
6. **Password security:** A password management policy exists, is automated, and is enforced across the entire organization.
7. **Viewable file extensions:** All computers are configured to show file extensions (i.e., .doc) and therefore allow users to see a possible executable file (i.e., .exe) and reduce the chance of someone accidentally opening a malicious hacker file.
8. **Email server controls:** Beyond user-level controls, there are up-to-date antivirus controls and malware software protections on all email servers and (upstream) verified controls with the ISP.
9. **Managing plug-ins:** All use of java and flash (and other) plug-ins are known and managed with the most recent updates.
10. **Limiting connectivity:** The most critical data are kept on a private network, not connected to the Internet.

Start with a conversation, then commit, then continue.

	Readiness To Defend and Protect										
	LOW			MED				HIGH			
	1	2	3	4	5	6	7	8	9	10	
Backup and Recovery: All systems and data are cataloged, ranked as critical priority 1-2-3, and a full backup system is in place and tested (along with recovery times) regularly.	1	2	3	4	5	6	7	8	9	10	***Best Practice:*** Start with a critical asset inventory. Then rank each (1, 2, 3) in terms of business criticality. Then, determine how long your business can tolerate any of the systems out of service (in terms of hours or days). Build and test a backup and recovery plan (with clear restore and recovery points) to mitigate this threat and restore operations.
Segmented Network Access: Critical data are segmented (separated) from single points of access so that if or when a breach occurs the data accessed is limited.	1	2	3	4	5	6	7	8	9	10	***Best Practice:*** Dynamic control or single point of control access is used across the network based on user and 'zone' of priority data.
Detection Systems: In addition to traditional firewalls, ransomware protection software and (early) detection system protocols are in place and tested regularly.	1	2	3	4	5	6	7	8	9	10	***Best Practice:*** Start with proper firewall management and then expand to additional hardware, anti-malware and ransom software, and people for perimeter protection.

1. **Full system inventory:** A list of all assets and devices, including APIs, software programs, and other tools (local and in the cloud) is available and regularly updated.
2. **Backup and recovery system:** All systems and data are cataloged and ranked as critical priority 1-2-3, and a full back up system is in place and tested (along with recovery time) regularly.
3. **Segmented network access:** Critical data are segmented (separated) from single points of access so that if or when a breach occurs the data that are accessed is limited.
4. **Detection systems:** In addition to traditional firewalls, ransomware protection software and (early) detection system protocols are in place and tested regularly.
5. **Trained workforce:** Regular security awareness training (pre-scheduled and "surprise" attacks) is mandatory and integrated into the business culture with a mindset of "see something, say something."
6. **Password security:** A password management policy exists, is automated, and is enforced across the entire organization.
7. **Viewable file extensions:** All computers are configured to show file extensions (i.e., .doc) and therefore allow users to see a possible executable file (i.e., .exe) and reduce the chance of someone accidentally opening a malicious hacker file.
8. **Email server controls:** Beyond user-level controls, there are up-to-date antivirus controls and malware software protections on all email servers and (upstream) verified controls with the ISP.
9. **Managing plug-ins:** All use of java and flash (and other) plug-ins are known and managed with the most recent updates.
10. **Limiting connectivity:** The most critical data are kept on a private network, not connected to the Internet.

Continue to learn, mature.

1. Can you remotely access the security solutions that you use daily to monitor for malicious behavior on the network and end-user devices such as PCs?
2. Can you remotely make configuration changes to your security solution set?
3. Can you remotely upgrade or patch your security solutions set?
4. Does a PC being located remotely change any of your containment or eradication processes?
5. Does the additional IP address added by VPN access affect your ability to map an IP address to a username?
6. If you are leveraging user behavior analysis does the fact that the user is now coming through VPN affect its ability to map the IP address to the end-user?
7. Can you remotely contain a server by isolating it from the network?
8. Can you remotely drop a network link to the offices in order to contain a potential malware outbreak (for example)?
9. Can you remotely contain a PC and conduct a forensic investigation?
10. Can you remotely access your critical servers and databases to investigate potential malicious behavior?
11. If everyone is working remotely, what IP traffic should you be seeing on the corporate network? This is important if someone has taken advantage of no one being at the facility.
12. Are your facilities monitored with security cameras? This is also important to ensure people are not accessing areas which are normally populated and restricted.
13. If you did have to send a team member into the building, have you walked through who that would be and the escalation and approvals that would be required to make that happen?
14. Can your team members answer calls to their work phone numbers remotely or do they need to forward their desk phones to their cell phone in case of an event?
15. Is there a delay or impact on any major security projects or initiatives that were underway? If they are critical, are there steps you can take to make progress to their implementation?
16. Have you notified your MSP partners?
17. Have you thought through how you would conduct daily updates and team meetings remotely?
18. Do you need to adjust any of your incident response plans to account for everyone being remote?
19. Does the network have the bandwidth to handle daily updates, i.e. antivirus, anti-malware, application patches going out to every PC remotely or do you need to stagger them throughout the day, or potentially days to account for the network limitations?
20. If any new hires are scheduled to start during this remote period, how will they be onboarded and the security surrounding their machine and her user ID be handled?
21. How will the chain of custody be handled if a PC forensics investigation is required?
22. For any security equipment that is on-premises, how are the environmental conditions being monitored temperature, humidity, etc.?
23. Should the worst case happen and one of your team members is unable to work, is your team sufficiently cross trained on the various security solutions so someone could take on that person's duties?
24. There are multiple members of your team who are no longer able to work. Do you have a Managed Security Services Provider (MSSP) on standby to take over their duties? o If yes, what order of priority?
25. Will on premise equipment managed by IT continue to be patched such as servers network devices, storage arrays, etc.?

Determine your business continuity.

The NACo Cybersecurity Leadership Academy

FREE

www.naco.org/cyberskills

timr@pdaleadership.com

SCHOLARSHIPS AVAILABLE

Two types of programs to choose from.

CYBERATTACK SIMULATION

weeklong reality-based, certified assessment that focuses on helping leaders of government organizations better protect and maintain their critical assets

CYBER LEADER ACADEMY

12-week online training facilitated to make existing leaders better and emerging leaders ready to address the most pressing cyber issues of today

Threat Prevention Strategies