

Treating cybersecurity like your home: Creating a better framework for cybersecurity

STRONGHOLD DATA LLC, A New Charter Technologies Company

Jason Rincker, CRO

jason.rincker@strongholddata.com

www.strongholddata.com



The Necessity Of Cybersecurity In The Nonprofit Sector



John Giordani Forbes Councils Member

Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Nov 8, 2022, 06:15am EST

John Giordani has extensive experience in cybersecurity and information assurance.



Nonprofits collect and store information about individuals who are often vulnerable and at-risk, like low-income families, children and the elderly. This makes their data a prime target for cybercriminals. Nonprofits often don't have the financial resources of for-profit companies, so they are especially vulnerable to cyberattacks. Nonprofits also collect sensitive information, such as social security numbers, that hackers can use for identity theft.

Cybersecurity for nonprofits is critical—these organizations provide essential services to their communities. In the event of a cyberattack that exposes the personal data of clients, the consequences are particularly significant.



MISSOURI'S STATE CAPITOL. IMAGE: LAUGHINGOUTLOUDICON VIA WIKIMEDIA COMMONS (CC BY-SA 3.0)

Jonathan Greig

August 9th, 2023

Government

News

Privacy



Missouri says some Medicaid health information was compromised in MOVEit breach

Missouri's Department of Social Services (DSS) this week became the latest state agency to confirm it had data stolen through a vulnerability affecting the MOVEit file transfer tool.

A DSS spokesperson would not say how many people were affected but said they will be sending notices to "all Missouri Medicaid participants and providers that were enrolled in May of 2023."



HCA Healthcare says data breach may affect 11 million patients in 20 states, including Kansas and Missouri

Share   



Updated: 9:55 AM CDT Jul 13, 2023

Infinite Scroll Enabled ☐

AP Associated Press

 Nick Sloan

COVERING KANSAS & MISSOURI

HCA HEALTHCARE DATA BREACH

▶ Overland Park Regional

▶ Menorah Medical Center

▶ Research Medical Center

▶ Full list at [KMBC.com](https://www.kmbc.com)






KMBC



Coverage You Can
Count On

▶ WATCH NOW

HOME ▾

NEWS ▾

WEATHER ▾

SPORTS ▾

WHAT'S ON

KOMU 8 CARES ▾

MU Health Care reveals patient data breach

Kevin Utz, Columbia Missourian May 18, 2023



Listen to this article now

⌕ Powered by **Trinity Audio**



1.0x

00:00

01:21

MU Health Care said it is mailing notifications to patients whose medical records may have been improperly accessed by a workforce member.



MU Health Care said in a news release Wednesday that it learned on March 20 that the individual had been accessing health information in the electronic medical record (EMR) inappropriately.

The agency immediately began an investigation and suspended the workforce member's access to the records.

The release said that the investigation revealed that the workforce member used the EMR to improperly access 736 records between July 2021 and March.

Current

65



K-12 Cybersecurity News

Illuminate Data Breach Spreads to Fifth State as Oklahoma City Notifies Parents

By Kristal Kuykendall | 05/17/22

Editor's Note: THE Journal has published an updated list of all K-12 schools nationwide known to be impacted by the Illuminate Education data breach.

Oklahoma City Public Schools has added its 34,000 students to the growing list of those impacted by the Illuminate Education data breach that occurred during a January cyberattack — the first in Oklahoma known to have been among the K-12 schools and districts whose private student data was compromised within Illuminate's systems.



NPR in Kansas City

A group of hackers has hit hundreds of hospitals, including in Missouri. The effects last years.

Side Effects Public Media | By Farah Yousry

Published March 30, 2023 at 3:00 AM CDT



▶ LISTEN • 4:25

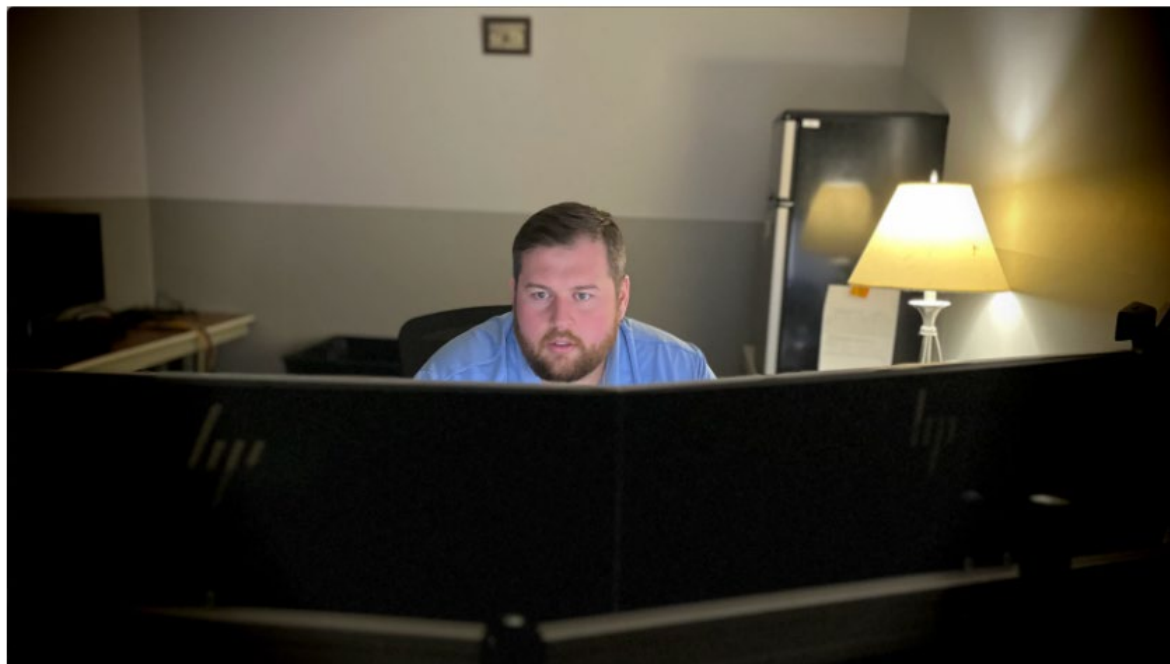




IMAGE: DERHAI VIA WIKIMEDIA COMMONS (CC BY-SA 3.0)

Jonathan Greig

April 26th, 2023

Briefs

Cybercrime



Truman State University slowly recovering from 'cybersecurity virus attack'

Truman State University in Kirksville, Missouri said it is in the process of recovering from a "cybersecurity virus attack" last week that forced it to shut down the campus network and order all school-issued devices to be turned off.

IEWS

Third-Party Data Breach Impacts 271K at Oklahoma Healthcare Administrative, Tech Services Company

Avem Health Partners said it was evaluating its vendor relationships after a third-party data breach potentially exposed patient information.



By Jill McKeon



December 22, 2022 - Oklahoma-based Avem Health Partners, which provides administrative and technology services to healthcare organizations, **notified** 271,303 individuals of a healthcare data breach that occurred at 365 Data Centers, a vendor used by a third-party service provider utilized by Avem.

BUSINESS > AIRLINES

Holiday meltdown exposes Southwest Airlines' technology woes

Corporate and union leaders at Dallas-based Southwest Airlines have talked about upgrading technology to avoid massive cancellation events.



A woman walks past a flight status board at Dallas Love Field airport in Dallas on Dec. 22. (Elias Valverde II / Staff Photographer)

By [Kyle Arnold](#) and [Natalie Walters](#)

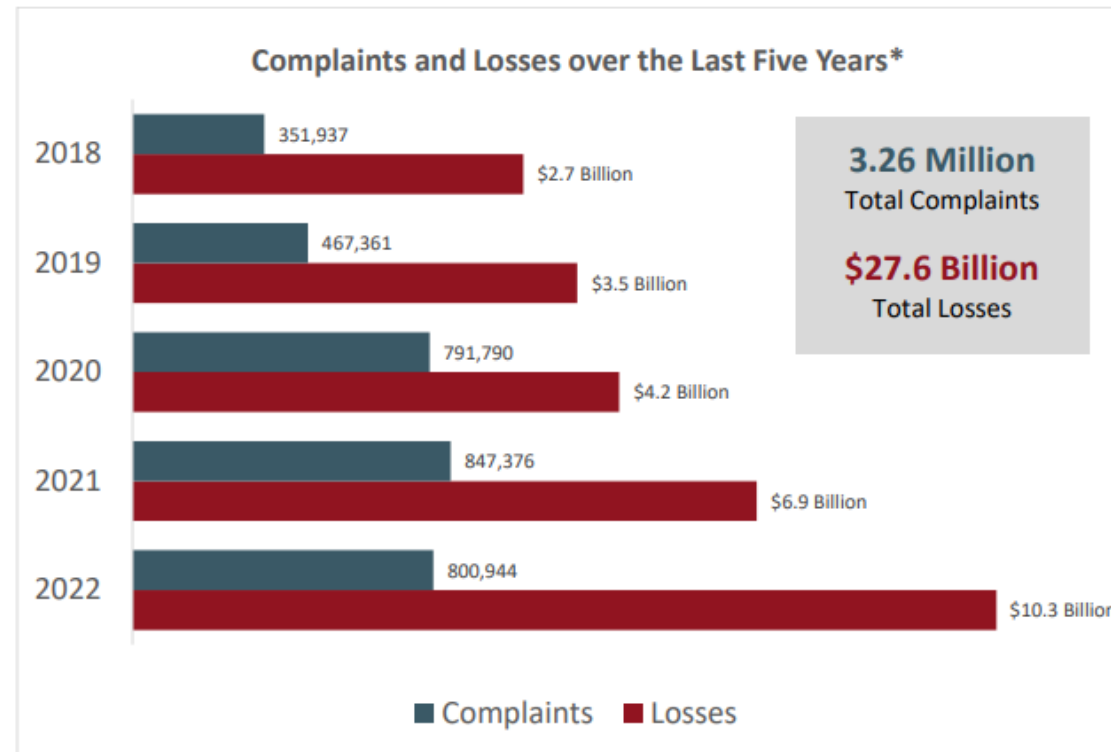
11:00 AM on Dec 29, 2022



IC3 COMPLAINT STATISTICS

LAST FIVE YEARS

Over the last five years, the IC3 has received an average of 652,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.³



OVERALL STATE STATISTICS continued

Total Victim Losses by State*					
Rank	State	Loss	Rank	State	Loss
1	California	\$2,012,806,866	30	Kansas	\$58,149,297
2	Florida	\$844,972,494	31	Kentucky	\$57,045,801
3	New York	\$777,099,358	32	Louisiana	\$55,696,565
4	Texas	\$763,140,903	33	South Dakota	\$48,072,730
5	Georgia	\$322,638,566	34	Puerto Rico	\$47,424,485
6	New Jersey	\$284,590,029	35	Arkansas	\$46,230,114
7	Illinois	\$266,742,489	36	Iowa	\$42,806,846
8	Pennsylvania	\$250,903,241	37	Delaware	\$40,980,800
9	Alabama	\$247,930,058	38	Idaho	\$40,323,594
10	Arizona	\$241,191,959	39	Hawaii	\$35,776,983
11	Washington	\$240,923,860	40	District of Columbia	\$33,668,057
12	Massachusetts	\$226,202,504	41	New Mexico	\$32,941,959
13	Maryland	\$217,880,447	42	New Hampshire	\$29,322,824
14	Virginia	\$205,462,224	43	Nebraska	\$28,659,814
15	Ohio	\$180,091,279	44	Mississippi	\$28,213,583
16	Colorado	\$178,389,862	45	Montana	\$22,252,737
17	Michigan	\$177,865,280	46	Rhode Island	\$21,827,037
18	North Carolina	\$175,454,536	47	Maine	\$21,403,477
19	Nevada	\$127,315,394	48	West Virginia	\$18,200,401
20	Missouri	\$118,365,728	49	Wyoming	\$17,980,141
21	Tennessee	\$113,713,897	50	Alaska	\$16,826,999
22	Oregon	\$109,917,253	51	Vermont	\$15,664,834
23	Wisconsin	\$108,909,445	52	North Dakota	\$14,279,199
24	Minnesota	\$103,771,677	53	Guam	\$2,712,088
25	South Carolina	\$100,256,530	54	Northern Mariana Islands	\$1,950,513
26	Connecticut	\$99,937,935	55	U.S. Minor Outlying Islands	\$960,281
27	Utah	\$98,840,388	56	Virgin Islands, U.S.	\$826,913
28	Indiana	\$73,678,120	57	American Samoa	\$127,716
29	Oklahoma	\$66,517,159			

FORBES > LEADERSHIP > LEADERSHIP STRATEGY

The 10 Biggest Risks And Threats For Businesses In 2023

Edward Segal Senior Contributor @
I cover crisis-related news, issues and topics.



Jan 1, 2023, 06:03am EST

- ▶ Recession
- ▶ Interest Rates
- ▶ Labor Shortage
- ▶ Rapidly Changing Market Trends
- ▶ Supply Chains
- ▶ Cybersecurity
- ▶ Damage to Reputations
- ▶ Inability to Reach Target Audiences
- ▶ Mental Health Issues in the Workplace
- ▶ Lack of Succession Planning

If you purchase via links on our site, we may receive **affiliate commissions**.

[Home](#) » [News](#)

Southwest Airlines sued for outdated technology



Stefanie Schappert, Senior Journalist

Updated on: 13 January 2023



Image by Shutterstock



Southwest Airlines is accused of ignoring "serious risks" associated with its outdated technology infrastructure and support systems, considered critical to the performance, reliability, and security of airline operations, as stated in a new lawsuit.

*in Newswire**Published on April 18, 2023*

Oklahoma City University Responsible for July 2022 Data Breach, Class Action Says

by **Kelly Mehorter**[➤ SHARE](#)[View Comments](#)

Ruskiewicz v. Oklahoma City University

[Read Complaint](#)

FILED: APRIL 10, 2023 ♦ § 5:23-CV-00303

A proposed class action claims Oklahoma City University failed to prevent a “foreseeable” data breach in July 2022.

DEFENDANT(S)

LAW(S)

STATE(S)

Oklahoma City University

Oklahoma

[i](#) New to ClassAction.org? Read our Newswire Disclaimer

A proposed class action claims Oklahoma City University failed to prevent a “foreseeable” data breach in July 2022.

Case Spotlight

Camp Lejeune

Camp Lejeune residents now have the opportunity to claim compensation for harm suffered from contaminated water.

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023





THE WHITE HOUSE
WASHINGTON


March 1, 2023

Digital technologies today touch nearly every aspect of American life. The openness and connection enabled by access to the Internet are game-changers for communities everywhere, as we have all experienced throughout the COVID-19 pandemic. That's why, thanks to the Bipartisan Infrastructure Law, my Administration is investing \$65 billion to make sure every American has access to reliable, high-speed Internet. And when we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the Internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable, and secure. This National Cybersecurity Strategy details the comprehensive approach my Administration is taking to better secure cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of our digital future.

Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense. From the very beginning of my Administration, we have moved decisively to strengthen cybersecurity. I appointed senior cybersecurity officials at the White House and issued an Executive Order on Improving the Nation's Cybersecurity. Working in close cooperation with the private sector, my Administration has taken steps to protect the American people from hackers, hold bad actors and cybercriminals accountable, and defend against the increasingly malicious cyber campaigns targeting our security and privacy. And we've worked with our allies and partners around the world to improve our capacity to collectively defend against and respond to cyber threats from authoritarian states that go against our national interests.

This strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace. It also takes on the systemic challenge that too much of the responsibility for cybersecurity has fallen on individual users and small organizations. By working in partnership with industry, civil society, and State, local, Tribal, and territorial governments, we will rebalance the responsibility for cybersecurity to be more effective and more equitable. We will realign incentives to favor long-term investments in security, resilience, and promising new technologies. We will collaborate with our allies and partners to strengthen norms of responsible state behavior, hold countries accountable for irresponsible behavior in cyberspace, and disrupt the networks of criminals behind dangerous cyberattacks around the globe. And we will work with the Congress to provide the resources and tools necessary to ensure effective cybersecurity practices are implemented across our most critical infrastructure.

As I have often said, our world is at an inflection point. That includes our digital world. The steps we take and choices we make today will determine the direction of our world for decades

The background of the slide features a hand holding a magnifying glass, focusing on a complex network diagram. The network consists of numerous nodes connected by lines, creating a web-like structure. The overall color palette is dark blue and grey, with a semi-transparent white box containing the text.

How Are You Keeping Your
Organization Out of the
Headlines?

Framework Functions

Functions
Identify
Protect
Detect
Respond
Recover

What processes and assets need protection?

How are we protecting our networks and data?

What are our capabilities for detecting a cyber attack?

What are our capabilities for responding to an attack?

What are our capabilities for returning to normal operations?



Homeland
Security



Security Strategy

PROTECT

DETECT

RESPOND

NIST Security Framework

PROTECT	DETECT	RESPOND
Doors and Windows	Alarm	Dog
Locks	Motion Sensor	Baseball Bat
Fence	Doorbell Camera	Police
Yard Signs	Neighborhood Watch	Insurance

Ten Activity Channels for Breach Response



-Peter Sloan,
Information Governance Group

Cyber Resilience

CYBERSECURITY

BUSINESS CONTINUITY, INCIDENT RESPONSE,
& CRISIS MANAGEMENT



IDENTIFY



PROTECT



DETECT



RESPOND



RECOVER

TECHNOLOGY

PEOPLE

PROCESS

ASSUME BREACH

LEFT OF

BOOM

RIGHT OF

Components of a Well-Designed Security Solution for Your Business



Security Assessment



Security Awareness



Passwords



DNS Protection



Mobile Device Security



Advanced Endpoint Detection & Response



SIEM / Log Management



Dark Web Research



Backup



Computer Updates



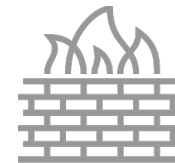
Spam Email



Multi-Factor Authentication



Encryption



Firewall



Cyber Insurance

Three Options when it comes to Risk



Assuming the Risk



Area One

Backups



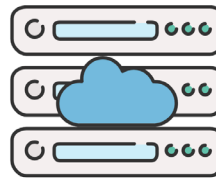
Area Two

Security Awareness
and Training



Area Three

Email Security



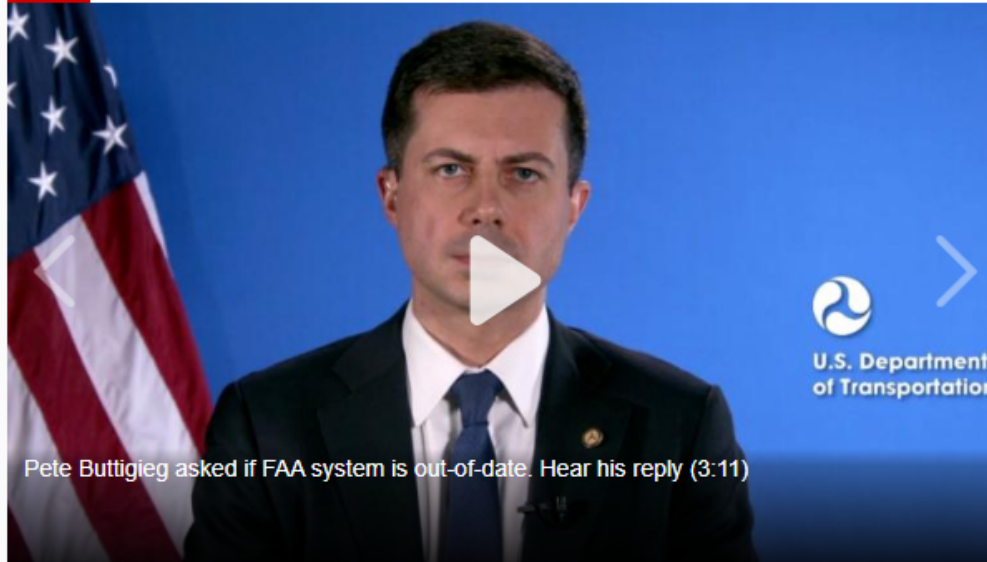
Area Four

Protecting Endpoints



Area Five

Network Security



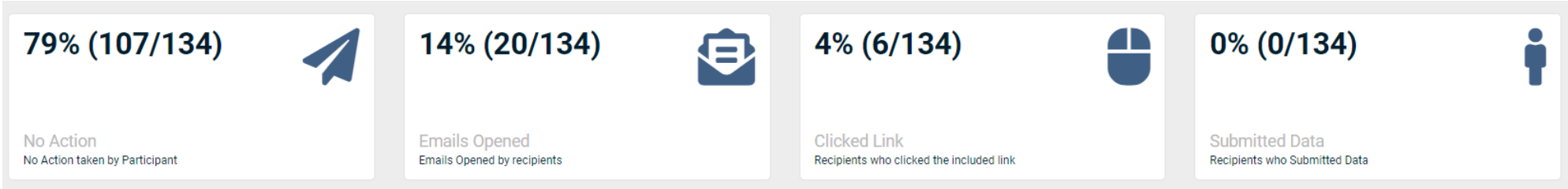
A corrupt file led to the FAA ground stoppage. It was also found in the backup system

Gregory Wallace and Pete Muntean, CNN • Updated 12th January 2023

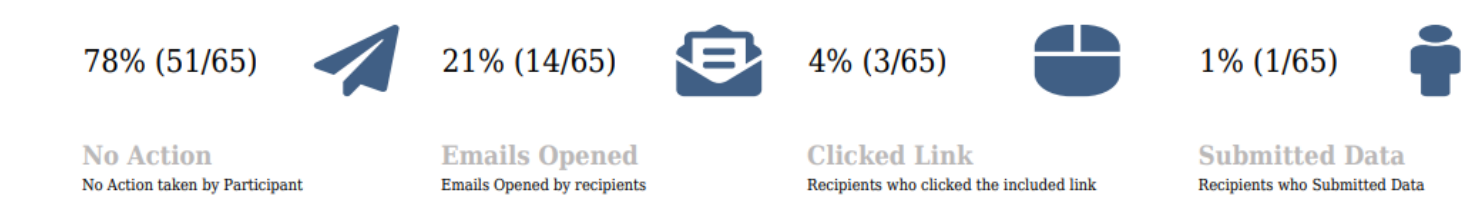


(CNN) — Officials are still trying to figure out exactly what led to the Federal Aviation Administration system outage on Wednesday but have traced it to a corrupt file, which was first reported by CNN.

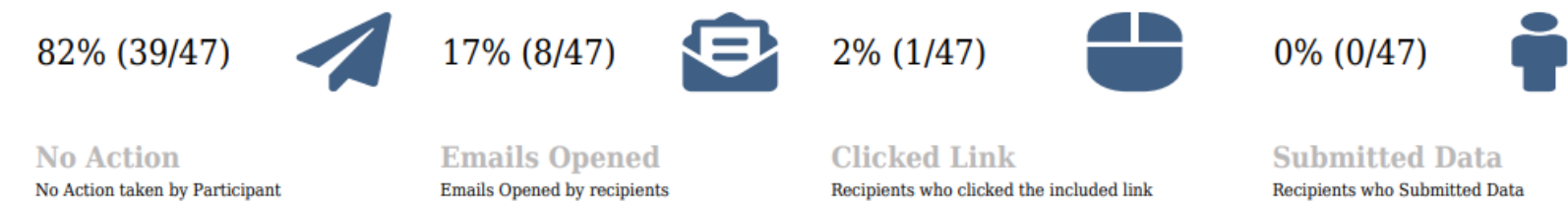
Spring 2023 Campaign



Fall 2022 Campaign



Summer 2022 Campaign



Three Options when it comes to Risk



MULTI FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing e-mail through a website or cloud based service. ☐ Yes ☐ No
☐ Email is not web based
2. Multi-factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☐ Yes ☐ No
3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:
- All internal & remote admin access to directory services (active directory, LDAP, etc.). ☐ Yes ☐ No
 - All internal & remote admin access to network backup environments. ☐ Yes ☐ No
 - All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.). ☐ Yes ☐ No
 - All internal & remote admin access to the organization's endpoints/servers. ☐ Yes ☐ No
4. The signer of this form has done so with the assistance of the person in charge of IT security. ☐ Yes ☐ No

Executive Officer Signature:

X

Name, Title, and email address:

Date (month/dd/yyyy):

Executive Officer is defined as the applicant's chief executive officer, chief financial officer, chief information security officer, risk manager, in-house general counsel, or the functional equivalent.

2. IT DEPARTMENT

This section must be completed by the individual responsible for the Applicant's network security. As used in this section only, "you" refers to the individual responsible for the Applicant's network security.

a. Who is responsible for the Applicant's network security?

Name:

Title:

Phone:

Email address:

IT Security Designation(s):

b. The Applicant's network security is: ☐ Outsourced ☐ Managed internally/in-house

c. How many IT personnel are on your team?

d. How many dedicated IT security personnel are on your team?

By signing below, you confirm that you have reviewed all questions in Sections 3 through 5 of this supplemental application regarding the Applicant's security controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to receiving direct communications from the Insurer and/or its representatives regarding potentially urgent security issues identified in relation to the Applicant's organization.

Print/Type Name:

Signature:

Three Options when it comes to Risk



Annual Information Security Risk Assessment

Annual Information Security Risk Assessment

Standard Assessment

My organization uses anti-virus and anti-spyware (malware) software:

- ☐ I am not aware of what kind of software we use
- ☐ We do not use this type of software
- ☐ We have it on some computers
- ☐ We have it on all computers but it is not updated on a regular basis and I question the quality of the product
- ☐ We update our software and scan all computers daily with a quality product

My organization secures our internet connection with a hardware firewall:

- ☐ I am not aware if we have a hardware firewall
- ☐ We do not use a hardware firewall
- ☐ We have a hardware firewall but I am not sure on its quality
- ☐ We have a commercial grade hardware firewall
- ☐ We have a commercial grade hardware firewall that has all default security settings changed

My organization has a software firewall on all computers:

- ☐ I am not aware if we have any software firewalls
- ☐ We do not use a software firewall
- ☐ We have a software firewall installed on a few computers
- ☐ We have a software firewall installed on all computers
- ☐ We have a commercial grade software firewall installed on all computers

Advanced Assessment

My organization trains our employees on security concerns regarding email attachments and emails requesting sensitive information:

- ☐ I am not aware of what training on email security threats is done
- ☐ We do not provide any training
- ☐ We casually discuss email security concerns with employees using email
- ☐ We require employees using email to watch webinars, read articles, or go to seminars covering email security
- ☐ We train employees when hired and on a regular basis about email security

My organization trains our employees on security concerns regarding web links in email, instant messages, and social media:

- ☐ I am not aware of what training on issues with web links in email, instant messages, and social media is done
- ☐ We do not provide any training
- ☐ We casually discuss issues with web links in email, instant messages, and social media with employees
- ☐ We require employees using the internet to watch webinars, read articles, or go to seminars covering web links in email, instant messages, and social media
- ☐ We train employees when hired and on a regular basis about issues with web links in email, instant messages, and social media

My organization trains our employees on security concerns regarding popup windows:

- ☐ I am not aware of what training on popup window threats is done
- ☐ We do not provide any training
- ☐ We casually discuss popup window concerns with employees using the internet
- ☐ We require employees using the internet to watch webinars, read articles, or go to seminars covering popup windows
- ☐ We train employees when hired and on a regular basis about threats from popup windows

THREE WAYS TO MONITOR VENDORS

1. **Vet vendors before hiring.** Assess cyber risk for every third party before working with them.
2. **Full Vendor Record Keeping.** Have full and clear documentation of every vendor and their vendors.
3. **Continuous Information.** Stay informed of the cyber posture of every vendor. The cybersecurity risk and threat landscape is constantly evolving, which requires constant updates.

Vendor Management



Search Security

TOPIC ▼
Compliance

S



NEWS

Biden issues cybersecurity guidance for software vendors

The guidance is an extension of President Biden's cybersecurity executive order from 2021 and includes new requirements for software deployed in federal agencies.



By Alexander Culafi, News Writer

Published: 14 Sep 2022



The White House released guidance Wednesday as an extension of a cybersecurity-focused executive order President Biden signed last year.

Biden signed "Improving the Nation's Cybersecurity" on May 12, 2021, outlining plans to [modernize the United States' cybersecurity posture](#) and implement technologies like multifactor authentication. One piece of the order referenced plans to provide guidelines for the software purchased and deployed within government networks; Wednesday's [memorandum](#) comprises these guidelines.

Biden's cybersecurity guidance requires that before using new software, federal government agencies must obtain a self-attestation form from the software producer confirming that the product is compliant with security guidance from [NIST](#). This guidance is referenced in the [executive order](#) and includes NIST's Secure Software Development Framework and Software Supply Chain Security Guidance.

Depending on the agency, the software producer might also be required to prove compliance through [artifacts](#) such as a [software bill of materials](#). In addition, the producer might be required to provide evidence that it participates in a vulnerability disclosure program.

Though the executive order and guidelines do not legally compel private vendors to release secure, compliant software, DeRusha said action was necessary in the wake of the SolarWinds supply chain attack in 2020, which led to breaches at several federal agencies.

"This incident was one of a string of cyber intrusions and significant software vulnerabilities over the last two years that have threatened the delivery of Government services to the public, as well as the integrity of vast amounts of personal information and business data that is managed by the private sector," DeRusha said in his statement.

STRATEGIC OBJECTIVE 3.3: SHIFT LIABILITY FOR INSECURE SOFTWARE PRODUCTS AND SERVICES

Markets impose inadequate costs on—and often reward—those entities that introduce vulnerable products or services into our digital ecosystem. Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance. Software makers are able to leverage their market position to fully disclaim liability by contract, further reducing their incentive to follow secure-by-design principles or perform pre-release testing. Poor software security greatly increases systemic risk across the digital ecosystem and leave American citizens bearing the ultimate cost.

We must begin to shift liability onto those entities that fail to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot

Selecting Vendors for Organizations

12 Key Questions

- **Areas of Expertise**
- **Security Mindset**
- **Compliance Standards**
- **Security Testing**
- **Transparency**
- **Collaboration**
- **Service Level Agreement**
- **Backup/Resilience**
- **Government/Policy**
- **Vendor Management**
- **Employee Training**
- **Data Retention and Destruction**

Summary

Public sector organizations must prioritize security and compliance when selecting vendors to avoid unnecessary risks. By asking these 12 questions, organizations can gain a better understanding of the vendor's capabilities and ensure they meet security and compliance requirements. This information will help public sector organizations select the right vendor and mitigate potential risks.

GOVERNMENT

Forthcoming SEC rules will trigger ‘tectonic shift’ in how corporate boards treat cybersecurity

The SEC’s proposal would require public companies to openly report serious cyberattacks, as well as explain who on their boards is responsible.



By [Tom McKay](#)

January 20, 2023 · 4 min read

The US Securities and Exchange Commission (SEC) will soon compel corporate boards to take cybersecurity seriously, whether they want to or not.

Under rules [first proposed in 2022](#) but expected to be finalized [as soon as April 2023](#), publicly traded companies that determine a cyber incident has become “material”—meaning it could have a significant impact on the business—must disclose details to the SEC and investors within four business days. That requirement would [also apply](#) “when a series of previously undisclosed, individually immaterial cybersecurity incidents has become material in the aggregate.”

The SEC’s rules will also require the boards of those companies to disclose significant information on their security governance, such as how and when it exercises oversight on cyber risks. That info includes identifying who on the board (or which subcommittee) is responsible for cybersecurity and their relevant expertise. Required disclosures will also include how often and by which processes board members are informed and discuss cyber risk.



**MSP INNOVATION
AWARDS NEW YORK 2022**

powered by **CHANNELPARTNERINSIGHT**



Jason Rincker

Director of Revenue

Jason.Rincker@strongholddata.com

www.strongholddata.com

