

Our ministry is to protect your ministry.

June 01, 2025

Risk Management 101— Privacy & Security

Partnering With You





Our Ministry: We protect the ministries of the Seventh-day Adventist[®] Church with insurance and risk management solutions. **I**

наражанын алтататын алтан төр

Information Security is a Universal Practice.



Our ministry is to *protect* your ministry.

MEDICAL REPORT

02:43 080

586 89403 253 684 01 99 RP 809

Cybersecurity Framework

- Identification
- Protection
- Detection
- Response
- Recovery



Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf



Why cybersecurity IT staff are so important

- 1. Proactive Threat Prevention and Mitigation
- 2. Enhanced Incident Response
- **3.** Compliance and Regulatory Requirements
- 4. Business Continuity and Reduced Risk
- 5. Reduced Financial and Reputational Damage



Multilayer Architectural Network



SEGMENTATION

Privacy & Security

Everyone's responsibility.

Awareness is the foundation of Risk Management

Adventist Risk Management, Inc.

Separation of Data Privileges

User and permissions management

User permissions can be assigned based on several criteria.

- 1. Role-based
- 2. Device-based
- 3. Location-based

User roles and access level descriptions

Administrative Rights



Types of Primary Data

Protected Health Information - PHI

Any data that could be used to identify an individual and relates to their physical and mental health, provision of healthcare or payment for that care.

Personally Identifiable Information - PII

Any data that can be used to identify a specific person, either directly or indirectly. This includes information like name, Government ID number, date of birth, address, or even a unique combination of data points.





PHI - Safeguards

Storage & Access

- 1. Medical records kept securely including encryption.
- 2. Medical records restricted to authorized personnel
- 3. Access to medical record storage areas are restricted
- 4. Policies and procedures to prevent unauthorized access, alteration, or deletion of information in charts



PHI - Safeguards

Disposal

Policies and procedures for securely disposing medical records

Accuracy

Procedures in place to ensure the accuracy and completeness of information in charts



PHI - Safeguards

Authorization

- Procedures in place to ensure that releases of information are properly authorized, with valid authorizations signed by the patient or their representative.
- 2. Procedures in place to verify the identity of individuals requesting information.
- 3. Policies and procedures to ensure that PHI is used or disclosed ONLY for permissible purposes and only to the extent necessary.



Let's take a Poll



Please select which data constitutes PHI.

- 1. Favorite color, alias, country
- 2. nickname, birth year, address
- 3. Last name, government ID#, telephone
- 4. Mother's maiden name, school, blood type





Home-based records (HBRs)

HBRs are health documents kept by individuals or their caregivers, rather than at a healthcare facility, to record a person's health history and service utilization.

- 1. Is it legible?
- 2. Is it accurate?
- 3. Do you train your patients or caregivers how to properly complete, add information and store HBRs?



"The question isn't if an attack will happen. The question is: are you ready?"

John Riggi
 National Advisor for
 Cybersecurity and Risk
 for the American
 Hospital Association



Awareness is the foundation of Risk Management

Password – Best Practices

For Device and application access

- Complex passwords
- Change routinely (at least every 90 days)
- Use letters, numbers, symbols
- Do not write your password
- Do not recycle passwords
- Do not share passwords
- Do not use the same password for multiple systems





12 Key Controls to Strengthen Your Security







Ę

12 Key Controls to Implement/Enhance



<u>.</u>

Multifactor Authentication (MFA) for remote access and admin/privileged access

Organizations should bolster their security through MFA, which requires at least two pieces of evidence (factors) to prove the user's identity and prevents attackers from effectively using stolen passwords. For example—a time sensitive pin code delivered through an app or via text message is often a second factor in addition to the user's password. Although no cybersecurity tools are perfect, MFA provides a substantial barrier to unwanted system access.

Endpoint Detection and Response (EDR)

It's important for companies to have up-to-date information about the security posture of any devices used by employees to receive or send corporate information, whether it's a laptop, desktop, or mobile device. EDR offers continuous monitoring and more advanced detection and automated response capabilities. The monitoring software will watch for any suspicious or irregular activities and can also facilitate rapid incident response across an organization's environment.

Secured, encrypted, and tested backups

Attackers exploit default device settings or misconfigurations. Controlling changes and aligning with an industry recognized security baseline to harden devices are critical to prevent attackers from reaching and exploiting their targets. Particularly, the use of RDP without VPN and MFA controls should be avoided.

O CA

Q

⊕

Privileged Access Management (PAM)

Privileged accounts are the keys to a network. When attackers compromise these accounts, they gain unlimited access to the network, increasing the likelihood of causing significant harm. Organizations can control for this by limiting the number of privileged accounts, using Just-in-time (JIT) elevation or vaults, and MFA. Many organizations implement PAM solutions that automate privilege and session management.

Email filtering and web security

Malicious links and files are still the primary way to insert ransomware, steal passwords, and potentially access critical systems. Today's first line of defense includes advanced technologies to filter incoming emails, block access to malicious sites or downloads (across both onsite and remote users), and test suspicious content in a secure "sandbox" environment.

Patch management and vulnerability management

Unpatched vulnerabilities remain a leading cause of intrusions into systems, with hundreds of vulnerabilities revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit vulnerabilities. Regular vulnerability scans and rapid patch management reduces the risk of cyberattacks on the network. Such actions allow organization to apply patches or uncover existing vulnerabilities and remediate before threat actors have a chance to exploit. Most underwriters expect to see an ability to apply critical patches within 72 hours across 95% of endpoints.



 $\langle \gamma \rangle$

MFA



Approve

Deny





12 Key Controls to Implement/Enhance



(

Cyber incident response planning and testing

An up-to-date Cyber Incident Response (CIR) plan with a trained team and experienced senior leadership provides efficiency and effectiveness in response to cyber incidents. Practice through tabletop exercises builds resiliency. When combined with backups, other business continuity plans, and monitoring of endpoints and the network, they significantly help mitigate impacts to business operations and help to protect an organization's reputation if an event does occur.

Cybersecurity awareness training and phishing testing

Attackers have taken advantage of COVID-19, a time when people were stressed to capacity, as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people. Employee cybersecurity training and phishing campaigns help ensure people remain aware of changes in the cyber environment and remain cautious.

Hardening techniques including Remote Desktop Protocol (RDP) mitigation

Attackers exploit default device settings or misconfigurations. Controlling changes and aligning with an industry recognized security baseline to harden devices are critical to prevent attackers from reaching and exploiting their targets. Particularly, the use of RDP without VPN and MFA controls should be avoided.



Adventist Risk Management[®] Inc

Logging and monitoring/network protections

Logging and monitoring network activities allows organization to identify, detect, and contain attacker's actions at an early stage. Automated tools can support human monitors as they track network events or anomalous user behavior. Efficient use of firewalls and other technologies requires well-defined strategies—network segmentation, intrusion detection and prevention systems, data leak prevention systems, etc.

\oplus

End-of-Life systems should be replaced or protected

End-of-life systems or technology become a risk because patches and other forms of security support are no longer offered. Once the software/technology is practically no supported it will be impacted by unfixable vulnerabilities. It needs to be either protected by compensating controls or ungraded to "supported" platforms.

0-0

Vendor/digital supply chain risk management

A significant proportion of attacks or incidents are initiated through the supply chain, whether it's a third-party access that is leveraged, a trusted software update that is compromised, a malicious code that comes through a library, or a critical service that becomes unavailable. Managing cyber supply chain by monitoring risks and dependencies and maintaining continuity plans goes a long way in reducing the overall cyber risk exposure.

Cybersecurity Awareness Training



Adventist Risk Management, Inc., partners with NINJIO to provide our Cybersecurity awareness training.







Cyber Liability Policy







Ę

Cyber Liability Policy Added Services

- 1. Computer Forensic Services
- 2. Breach response
- 3. Negotiation and payment of a ransomware demand
- 4. Data restoration
- 5. Breach notification services to affected individuals
- 6. Legal services





Let's take a Poll



What is Ransomware?

- a type of malicious software designed to block access to a computer system until a sum of money is paid.
- 2. a cyberattack that floods a machine or network with false requests, making it unavailable to legitimate users.
- **3.** data that could be used to identify an individual and relates to their physical and mental health, provision of healthcare or payment for that care.
- 4. cyberattack where an attacker intercepts communication between two parties without their knowledge, inserting themselves into the conversation.







Case Study: Union – Retirement Fund

- 1. Error message in bank website
- 2. Employee got a call from bad actor impersonating the bank.
- 3. A pop-up window requested login information
- 4. Bank token security password was not sent or provided.

ΓΞ	6		
		F	
	-	-	



Case Study: NAD University

- 1. Bad actors infiltrated an employee's account.
- 2. Bad actors monitored the account for months to understand its systems and operations.
- 3. A ransomware attack completely disabled the network.
- 4. For TWO weeks, the university was locked out of its system.

Q		
) <u>.</u>	



FACTS

- 1. On average, organizations recover only 57% of compromised data after a cyber attack
- 2. 43% of data is permanently lost or damage after the ransom is paid.
- 3. Only 8% of people that suffered ransomware and paid get all their data back.

Top 10 Cyber Recovery Stats You Can't Ignore – Calamu.com





FACTS

- 1. Cyber Wars: Nation-states are leveraging Al-driven tactics, including disinformation campaigns and disruptive malware, to weaken systems and sow chaos globally.
- 2. Ransomware: Criminals are shifting from data encryption to extortion, with ransomware emerging as one of the most significant cyber threats to businesses worldwide in 2024
- 3. Infostealers. These malware attacks have surged by 58%, stealing credentials and sensitive data, impacting individuals and organizations alike

The State of Cyber Security 2025 - CheckPoint.com





What are the RED flags?

From: Demitris Barnwell <<u>dbarnwell@adventsitrisk.org</u>> Sent: Wednesday, April 30, 2025 10:44 AM To: Cc:

Subject: Re: FW: Adventist New Account Updated

Hello

Ę

Please find attached the ACH Bank information for processing payment to Adventist Risk going forward. Kindly confirm it is received and when payment will be expected.

Please let me know if you have questions.

Thank you,

Adventist Risk

Management[®] Inc.

Adventist Risk

Management[®] Inc.

?

Demitris Barnwell

Customer Service Representative Client Care

301-453-8896 DIRECT 240-268-5774 MOBILE DBarnwell@adventistrisk.org https://adventistrisk.org





What are the RED flags?

From: Demitris Barnwell <<u>dbarnwell@advent<mark>si</mark>trisk.org</u>>

ACH PAYMENT INSTRUCTIONS

Adventist Risk

Bank Name: Chase Bank Adventist Risk Management, Inc Account Number: 682571537 ACH Routing: 103000648

Please find attached the ACH Bank information for processing <mark>payment to Adventist Risk going forward</mark>. Kindly confirm it is received and when <mark>payment will be expected</mark>.





Online Safety Checklist



Adventist Risk Management[®] Inc. Adventist Risk Manugement; Inc.

Online Safety Checklist

Consecutory

Organization:	
Date:	
Inspector:	
Title:	

NOTE: The following list of inspections provides a form for identifying the "basic" cybersecurity items. This list is by no means a complete list of risk control exposures. A "No" response in the following topics may indicate a need for additional safety/risk management measures.

Administrative

Item	YES	NO	N/A	Description/Recommendation
1. There are written guidelines in place for:				
 protecting data 	\bigcirc	\bigcirc	\bigcirc	
confidentiality of data	\bigcirc	\bigcirc	\bigcirc	
 expectations of privacy 	0	0	\bigcirc	
monitoring privacy issues	\bigcirc	\bigcirc		
 limiting data success and use 	\bigcirc	\bigcirc	\bigcirc	
 password management and requirements 	0	0	\bigcirc	
 "bring your own device" (BYOD) 	\bigcirc	\bigcirc	\bigcirc	
 handling security incidents 	Õ	Õ	\bigcirc	
 social media posting and management 	\bigcirc	\bigcirc	\bigcirc	
 The conference or other legal entity has cyber insurance that covers the organization. 				
 There is a process for verifying third parties' security controls that have access to any personal data. 	\bigcirc	\bigcirc	\bigcirc	

Inventory

Item	YES	NO	N/A	Description/Recommendation
1. List of all hardware and software used.	\bigcirc	\bigcirc		
 All non-essential software has been removed from ministry devices. 	\bigcirc	\bigcirc	\bigcirc	
 Someone is assigned to track all ministry hardware and software annually. 	\bigcirc	0	0	
 Inventory of all technology assets with the potential to store or process information, regardless if connected to the network or not. 				

© 2020 Adventist Risk Management,* Inc.

FRM-OnlineSafety-Checklist-NADEN

em	YES	NO	N/A	Description/Re	commen	dation					
ks have passwords.	0	0	0								
passwords have been											
are configured with											
ld about their assword/account											
eparate administrator ints, permissions, and		0	Q								
inique and meet the	0	0						Online Safety Checklist Page 2 of 4			
cter alpna-numeric									100		
ntication (MFA or 2FA) on all accounts, which al security layer.		0									
network/data access sing the rule of least ants access to the level								escription/Recommendation			
lete approved actions. s have been reviewed	0	0	0								
ivileged access have ement and undergone a	0	0	0								
nave been deleted.	0	0	0								
/accounts have been re is documentation access. (Shared	Ŏ	Ŏ	Õ								
ermissions are	\bigcirc	0	0								Online Safety C
ment,* Inc.				FRM-Onli	neSafety-C	hecklist-NA	IDEN		5 NO	N/A	Description/Recommendat
ment,ª Inc.	0 4. U	onfirmed a	as part of the	FRM-Onli he inventory process. such as personal	neSafety-O	hecklist-NA	DEN		5 NO	N/A	Description/Recommendat
sment,* Inc.	o 4. U n ir	onfirmed i nauthorizi nobile devi iternal net	as part of the red devices, are resi works.	FRM-Onli he inventory process. such as personal tricted from accessing	neSafety-Cl	hecklist-NA	DEN		5 NO	N/A	Description/Recommendat
ament" Inc.	o 4. U nir	onfirmed a Inauthoriz Inobile devi Iternal net	as part of the ed devices, are rest works.	FRM-Onli ne inventory process. such as personal tricted from accessing	neSafety-O	heckiist-NA	DEN			N/A	Description/Recommendat
ment" Inc.	0 4. U n ir Awa	onfirmed i Inauthorizi nobile devi nternal net reness isers have	as part of th ad devices, s kes, are rest works. Item been trains	FRM-Onlik the inventory process such as personal tricted from accessing edieducated on the	YES	NO	DEN	Description/Recommendation	5 NO	N/A	Description/Recommendat
ment*inc.	Awa	onfirmed a inauthoriz oblie devi- nternal net reness isers have sks of inst he work of honping a	as part of the ad devices, sices, are rest works. Item been trained alling new 'the minist post etc.)	FRM-Onli ne Inventory process. such as personal tricted from accessing ed/educated on the software related to n the software related to n the	YES	NO	DEN	Description/Recommendation	5 NO	N/A	Description/Recommendat
wert," bc.	Awa 1. U 1. U 1. U 1. U 1. U 1. U 1. U 1. U	onfirmed i inauthorize oblie devi iternal net reness isers have sks of inst hopping a ill personn omputers	as part of the red devices, are rest works. Item been trained alling new ithe minist pps, etc.). el interacti receive cyb	FRM-Onlik he inventory process: such as personal tricted from accessing ed/educated on the software related to ry (e.g., games, chat, ing with ministry rescuritly awareness	YES	NO	N/A	Description/Recommendation			Description/Recommendat
ment [*] lnc	0 0 4. U n ir 1. U 1. U 1. U 1. U 1. U 1. U 1. U 1. U	onfirmed i inauthoriz nobile devi- ternal net sers have sks of inst- he work of hopping a II personn omputers aining at isers have isers have	as part of th ed devices, s ices, are rest works. Item alling new the minist pps, etc.). el interacti receive cyb least once o signed an a istru davis	FRM-ONI he investory process: such as personal initiated from accessing indeducated on the software related to ny (e.g., sames, chat, ny	YES	NO	N/A	Description/Recommendation			Description/Recommendat
ment*to:	0 4. U nir 1. U ri ti si 2. A 0 0 1. U nir 1. U 0 1. U 0 0 1. U 0 1. U 1. U 0 U 0 U 1. U 1.	onfirmed is inauthorizz obile devi ternal net reness isers have work of hopping a JI personn workers aining at i sers have sisses have aining at i sers have sisses min	as part of the rel devices, i ces, are rest works. Item been traine alling new the minist pps, etc.). el interacti receive cyb least once essigned an a istry device k Managemer	FBM-Onio helinewethy process: such as personal intered from accessing deducated on the onforware related to ny (e.g., games, chat, or presently avareness adviness.	YES	NO	N/A	Description/Recommendation			Description/Recommendat
ment*to:	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	onfirmed i nauthoriz ternal net reness sers have sks of inst sers	as part of the devices, are resident of the devices of the device of	THM ONL Intelligenteed on the constraints of the second on the second on the constraints of the second on the second on the constraints of the second on the second on the s	YES	NO	N/A	Description/Recommendation PRM-OblesSelety-Checkle-NADEM 11: MINADE INVESTIGATION OF the Comparison of the Company and the		N/A	Description/Recommendat
ment,* bo:	0 4. U 1. U 1. U 1. U 1. U 1. U 1. U 1. U 1	onfirmed i nauthoriz ternal net reness sers have ksk of inst hopping a ll person myputers aining at i tsers have sisses have sisses have sisses have	as part of th ed devices, ces, are resi works. Item been training ling new the minist ling new the minist	Inst-Onio the Instrument process: tacking periodic instruct from accessing instruct from accessing instruct from accessing instruction accessing instructi	YES O	NO		Description/Recommendation Description/Recommendation MARCOMINGSING Checkste MODM AMAGE MARCOMINGSING Checkste MODM AMAGEMENT			Description/Recommendat
ment*tac	0 4. U 9 1. U 1. U 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	onfirmed in authorize in authorize ternal net reness have kes of inst works of inst works of inst ining at a sters have ining at a sters have in the sters ining at a sters have in the sters ining at a sters have in the sters ining at a sters ining ining	is part of the devices, are resi executions of the ministry of the ministry of the ministry part of the ministry of the ministry of the ministry part of the ministry of the ministry of the ministry part of the ministry of the ministry of the ministry part of the ministry of the ministry of the ministry of the ministry part of the ministry of the ministry of the ministry of the ministry of the ministry of the ministry of the ministry of the ministry of the ministry of the ministry of the mi	Test-Could be intermediated by the second solution of the second second endeducated on the software related by (e.g., guesse, club, club, club, club, club, endeducated on the software related by (e.g., guesse, club,	YES O	NO	OCH	Description/Recommendation Description/Recommend			Description/Recommendat

Online Safety Checklist Page 2 of 4

Questions?





Assignment

Who performs your Cybersecurity functions at your institution?

Share your latest risk event or concern.



Adventist Risk Management, Inc.



This presentation and any materials distributed are general information which is fact or research based but should not, under any circumstances, be considered specific legal advice regarding a particular matter or subject. Please consult your local attorney if you would like to discuss how a local jurisdiction deals with any specific circumstances you may be facing. For risk management issues, please consult your ARM Account Executive or other risk management professional.

Copyright © 2025 Adventist Risk Management,[®] Inc. All rights reserved.

www.adventistrisk.org