Adventist Risk Management, Inc.

Our ministry is to protect *your ministry.*

June 01, 2025

Risk Management 101—
Privacy & Security

Partnering With You

Seventh-day Adventist® Church

Adventist Risk Management,® Inc.

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

Information Security is a Universal Practice.

Adventist Risk Management, Inc.

Our ministry is to *protect* your ministry.

Cybersecurity Framework

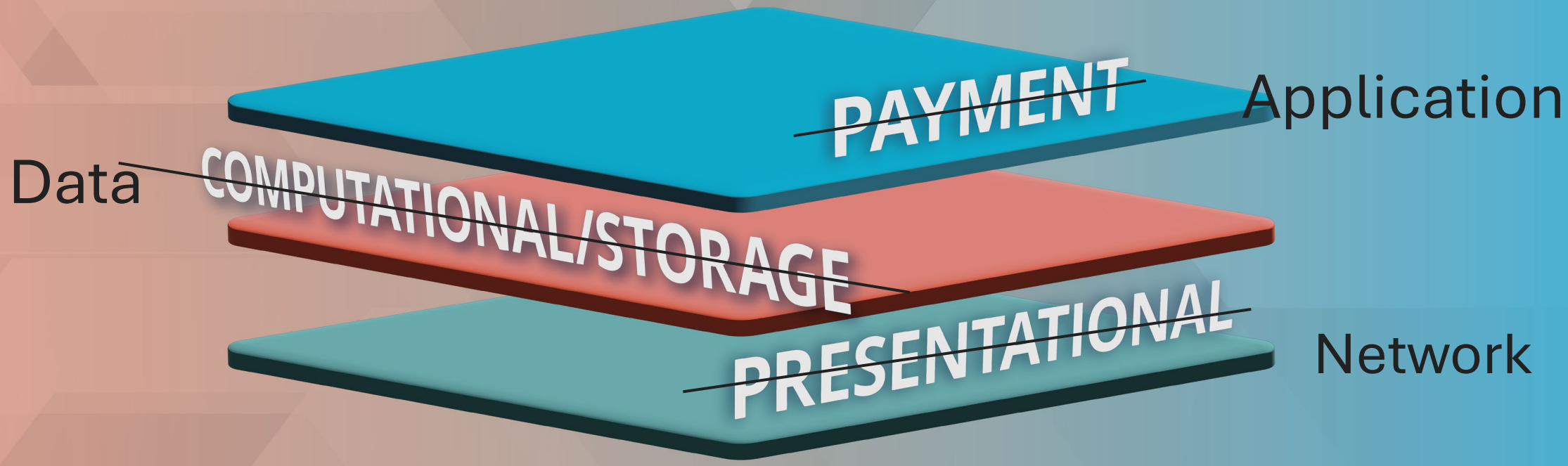
- Identification
- Protection
- Detection
- Response
- Recovery

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.

Adventist Risk Management, Inc.

Awareness is the foundation of Risk Management

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

1. 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

PHI - Safeguards

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

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

- Multifactor authentication for remote access and administrator/ privileged controls.
- Endpoint detection and response (EDR).
- Secured, encrypted, and tested backups.
- Privileged access management (PAM).
- Email filtering and web security.
- Patch management and vulnerability management.
- Cyber incident response planning and testing.
- Cybersecurity awareness training and phishing testing.
- Hardening techniques, including remote desktop protocol (RDP) mitigation.
- Logging and monitoring/network protections.
- End-of-life systems replaced or protected.
- Vendor/digital supply chain risk management.

Marsh

Adventist Risk Management, Inc.

Our ministry is to ***protect*** your ministry.

12 Key Controls to Implement/Enhance

Marsh

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.

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.

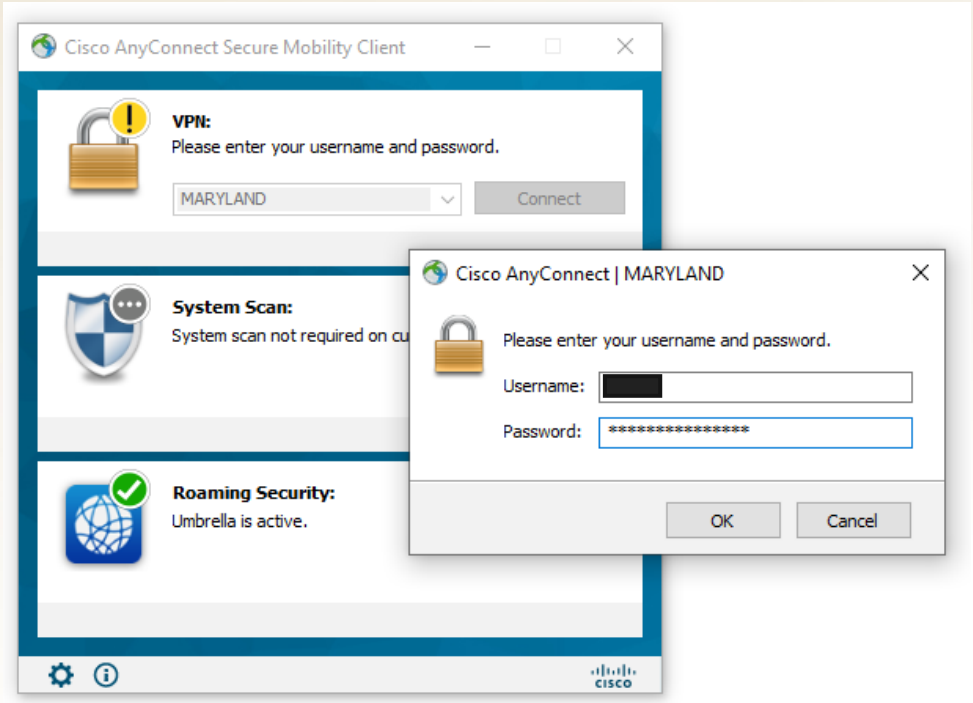
Email filtering and web security

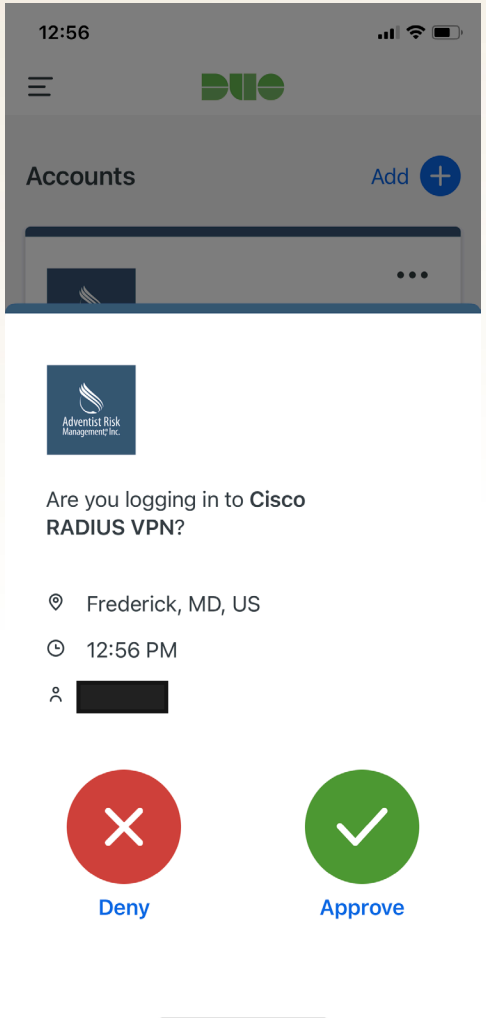
Malicious links and files are still the primary way to insert ransomware, steal passwords, and potentially access critical systems. Today's first line of defense includes advanced technologies to filter incoming emails, block access to malicious sites or downloads (across both onsite and remote users),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

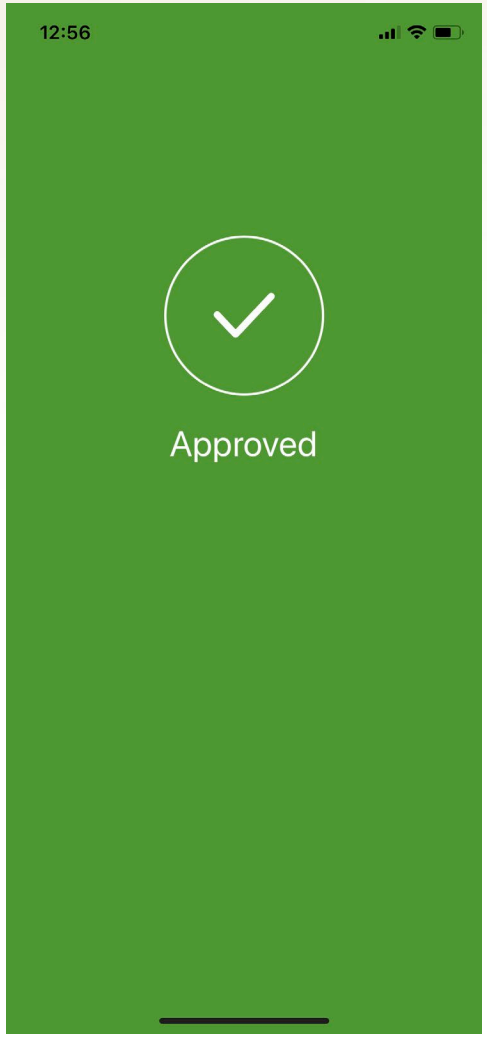
Patch management and vulnerability management

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.

MFA







Adventist Risk Management® Inc.

Our ministry is to ***protect*** your ministry.

12 Key Controls to Implement/Enhance

Marsh

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.

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.

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.

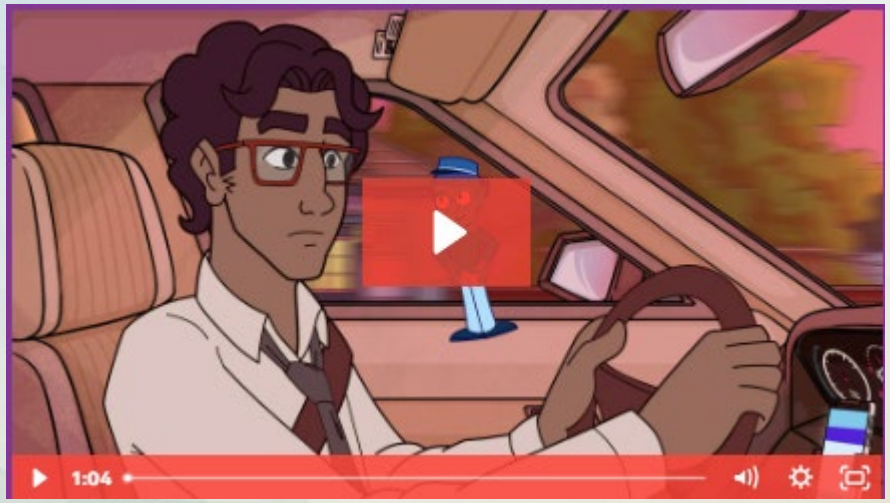
Vendor/digital supply chain risk management

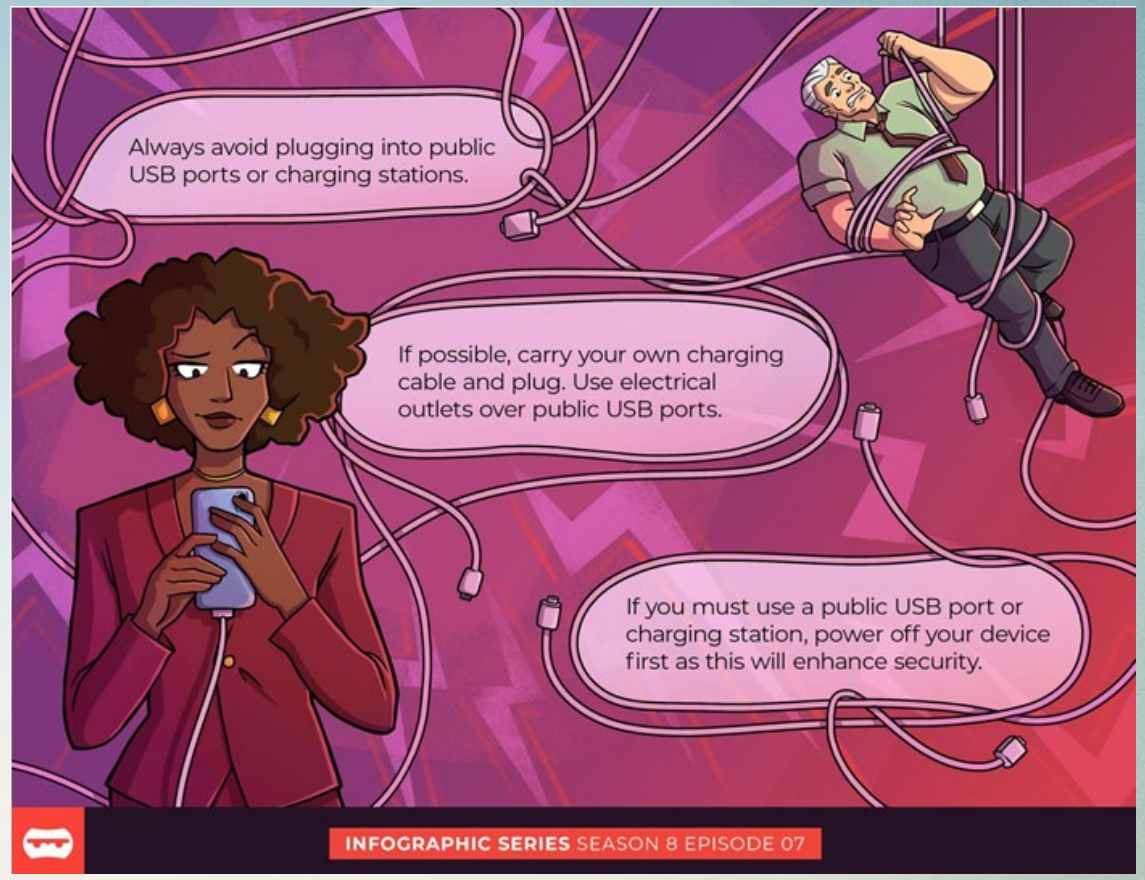
A significant proportion of attacks or incidents are initiated through the supply chain, whether it's a third-party access that is leveraged, a trusted software update that is compromised, a malicious code that comes through a library, or a critical service that becomes unavailable. Managing cyber supply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

Cybersecurity Awareness Training

NINJIO

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





Cyber Liability Policy

1 First Party

2 Third Party

3 eCrime

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?

1. 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:
Wiring Incident

$$$

South Heaven Union

ADRA
X

ADRA
M

$1,000

director@adracountrim.org

$199,000

Adventist Risk Management, Inc.

Our ministry is to ***protect*** your ministry.

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.

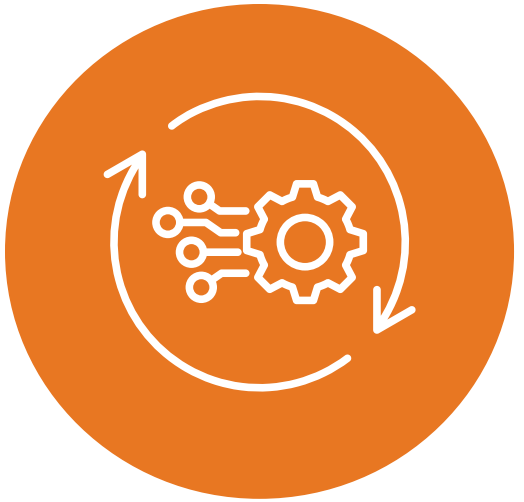
Case Study:
NAD University

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.

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 AI-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 <dbarnwell@adventsitrisk.org>
Sent: Wednesday, April 30, 2025 10:44 AM
To: [redacted]
Cc: [redacted]
Subject: Re: FW: Adventist New Account Updated

Hello [redacted]

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.

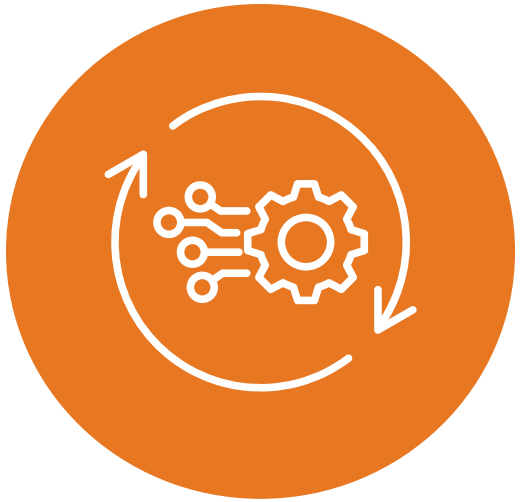
Please let me know if you have questions.

Thank you,

Adventist Risk Management, Inc.

Demitris Barnwell
Customer Service Representative
Client Care

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



Our ministry is to ***protect*** your ministry.

What are the RED flags?

From: Demitris Barnwell <dbarnwell@adventsitrisk.org>

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.

Adventist Risk Management, Inc.

ACH PAYMENT INSTRUCTIONS

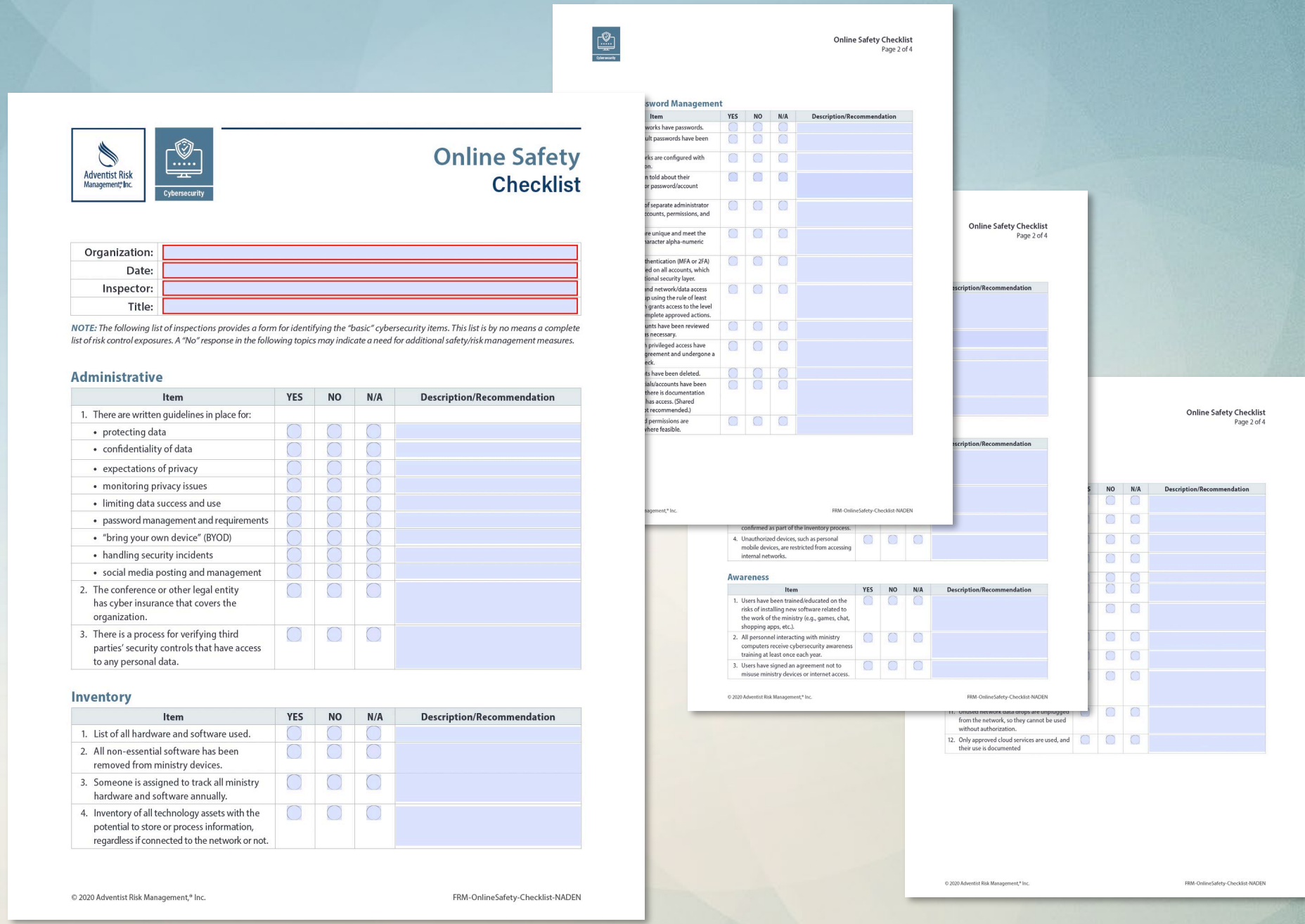
Bank Name: Chase Bank

Adventist Risk Management, Inc

Account Number: 682571537

ACH Routing: 103000648

Online Safety Checklist



Adventist Risk Management,® Inc.

Our ministry is to *protect* your ministry.

Questions?

Assignment

Who performs your Cybersecurity functions at your institution?

Share your latest risk event or concern.

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.

www.adventistrisk.org