The Fund

Third-Party Risk & Security Vetting in the Digital Age

Presented by:

Ron Frechette
Founder & CEO
GoldSky Security, LLC

GOLDSKY
CYBER SECURITY SOLUTIONS

PRESENTER

Ron Frechette, Founder & CEO

ron.frechette@goldskysecurity.com

o: (407) 853 8404 c: (904) 610 3420

Ron serves as Chief Evangelist Officer for GoldSky Security with over 10 years of experience directing Security Risk Assessment engagements and developing Cybersecurity Plans for various size companies across North America. Known to many as “The Cyber Coach”, he is constantly studying emerging cybersecurity trends and shares his knowledge through blogging platforms, local publications and speaking engagements across various industries.

Ron’s area of expertise has evolved from supporting large enterprise companies to helping small-midsize businesses with their IT security and compliance needs. He has assisted various companies in becoming compliant with frameworks such as FedRAMP, FISMA, GLBA, HIPAA/HITECH, HITRUST CSF, ISO27001, NIST CSF, NIST 800-53, 800-171, NERC-CIP, PCI DSS, SSAE 18 (SOC1), SOC2 and SOC3.

AGENDA

1. The Third-Party Risk & Security Vetting Trend

- What is Driving the Trend?
- Third-Party Data Breaches on the Rise
- Formal Notice of a Data Breach
- Cybersecurity Adoption Curve for SMBs
- The Fourth Revolution

2. The Cybersecurity Questionnaire

- Top 10 Security Questions
- Introduction to NIST
- ALTA Best Practices – Pillar 3
- Sample Reports
- Ethical Concerns-Practicing Due Care
- Florida State Law
- Top Threats to the Real Estate Industry

3. Adopting a Cybersecurity Framework

- Your Digital Footprint
- Objectives for Building a Cybersecurity Program
- Self-Assessment Resources
- Questions

The Third-Party Risk & Security Vetting Trend

WHAT IS DRIVING THE TREND?

Over the past decade, enterprise companies have invested millions of dollars in building highly secure and compliant infrastructures to avoid the risks of data theft, lawsuits, penalties for non-compliance and of most importance, brand damage and loss of business.

This has made it **more time consuming and difficult for cyber criminals to gain access** to large enterprise networks.

Cyber criminals are well aware of this which has caused them to shift their attack vectors towards third-party service providers in an effort to gain access to larger infrastructures. The Target Breach is a prime example.

Businesses are being forced to transform to ***the Digital Age way*** of conducting business or risk losing new and existing clients.

THIRD-PARTY DATA BREACHES ON THE RISE

2018 Third-Party Ecosystem Risk Study - Opus and the Ponemon Institute study in 2018 that surveyed more than 1,000 CISOs in US and UK.

Primary Objective - understand the challenges companies face in protecting sensitive information shared with third-party vendors. Third parties include any company whose employees or systems have access to a companies' systems or data (e.g. managed IT service providers, law firms, email providers, web hosting companies, subsidiaries, vendors, sub-contractors).

Some of the key findings revealed the following:

- 61% of US companies said they experienced a data breach caused by one of their vendors or third parties;
- 50% are unaware if supplier safeguards put in place are effective;
- 75% of organizations believe that third-party cybersecurity incidents are increasing;
- 16% attested they effectively mitigate third-party risk.

Conclusion: Third parties are one of the **fastest-growing risks to an organization's sensitive data**, yet less than half of all companies say managing third-party relationship risks is a priority.

These findings have put larger companies and their security auditors on high alert which is causing them to scrutinize the security practices of their current and future third-party service providers.

Source: https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party

FORMAL NOTICE OF A DATA BREACH

Dear Client:

Data privacy for our clients is at the center of our mission at X Law Group and we take seriously the confidentiality of the information we hold on your behalf. We regret to inform you that on September 01, 2018 we confirmed an unauthorized intrusion into our computer system. We took immediate action and are working closely with forensic experts and the FBI to investigate and address the situation.

While our investigation is ongoing, we have found evidence indicating that information such as company/customer names, addresses, email addresses, and dates of birth were potentially taken. In some cases the healthcare records, or social security numbers may also have been taken.

If you were a client of our company prior to July 2018, you may be affected. Our investigation is in its early stages, but we felt it was important to communicate what we know at this time. We regret any anxiety or frustration that this causes you and are committed to supporting you.

We are reaching out directly to those affected via mailed letters and are offering one year of free identity protection services, including credit monitoring for affected individuals. In this letter, we will also outline other steps you can take to protect your identity, as well as information on how to access the free identity protection services.

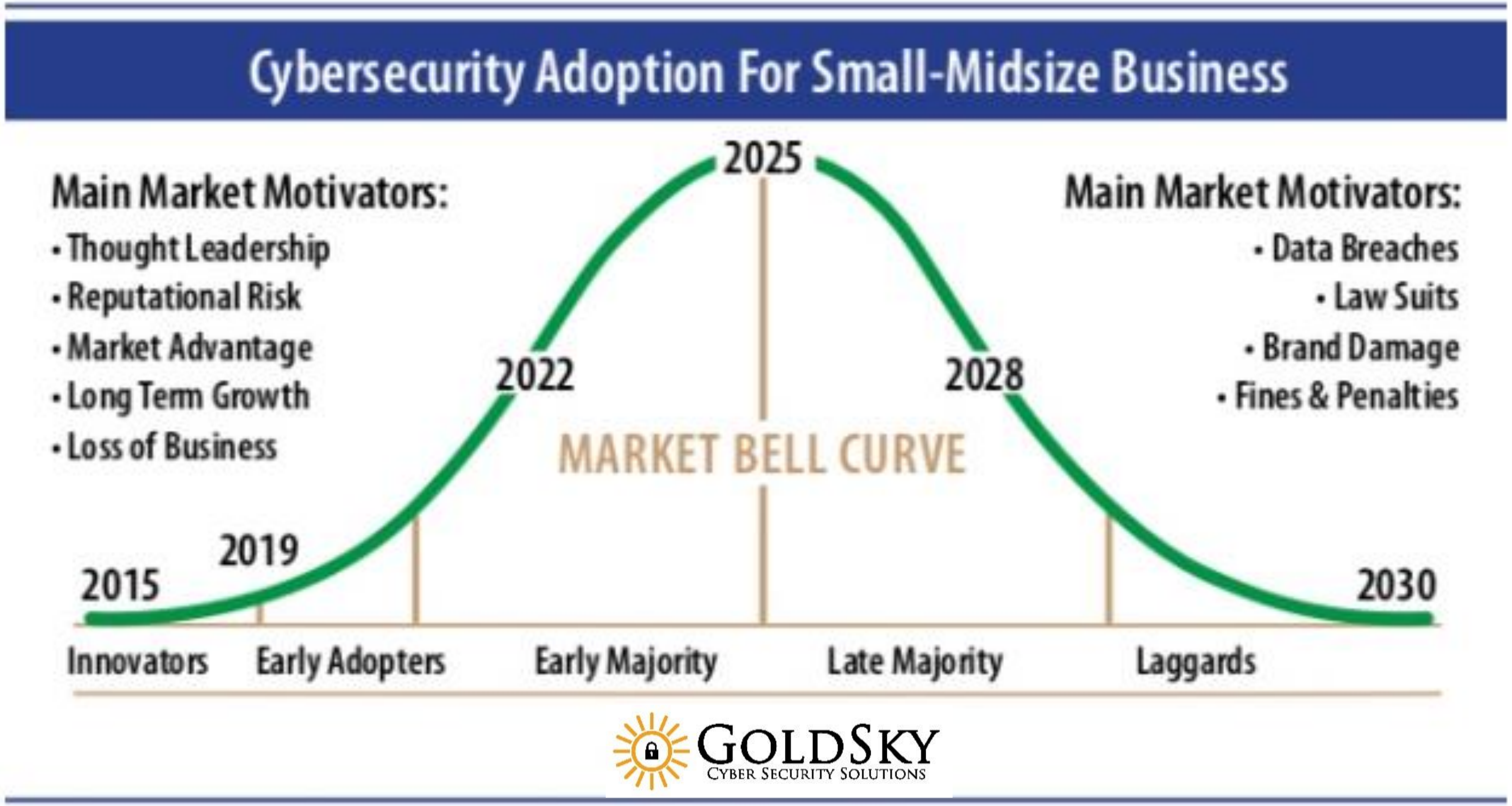
If you have any questions, we have established a dedicated call center, which can be reached by calling (844) 800-8080 between 9 a.m. and 9 p.m. ET, Monday-Friday.

Thank you for your patience and understanding as we work through our investigation and try to provide you the best information and support that we can. We will share further information as we are able.

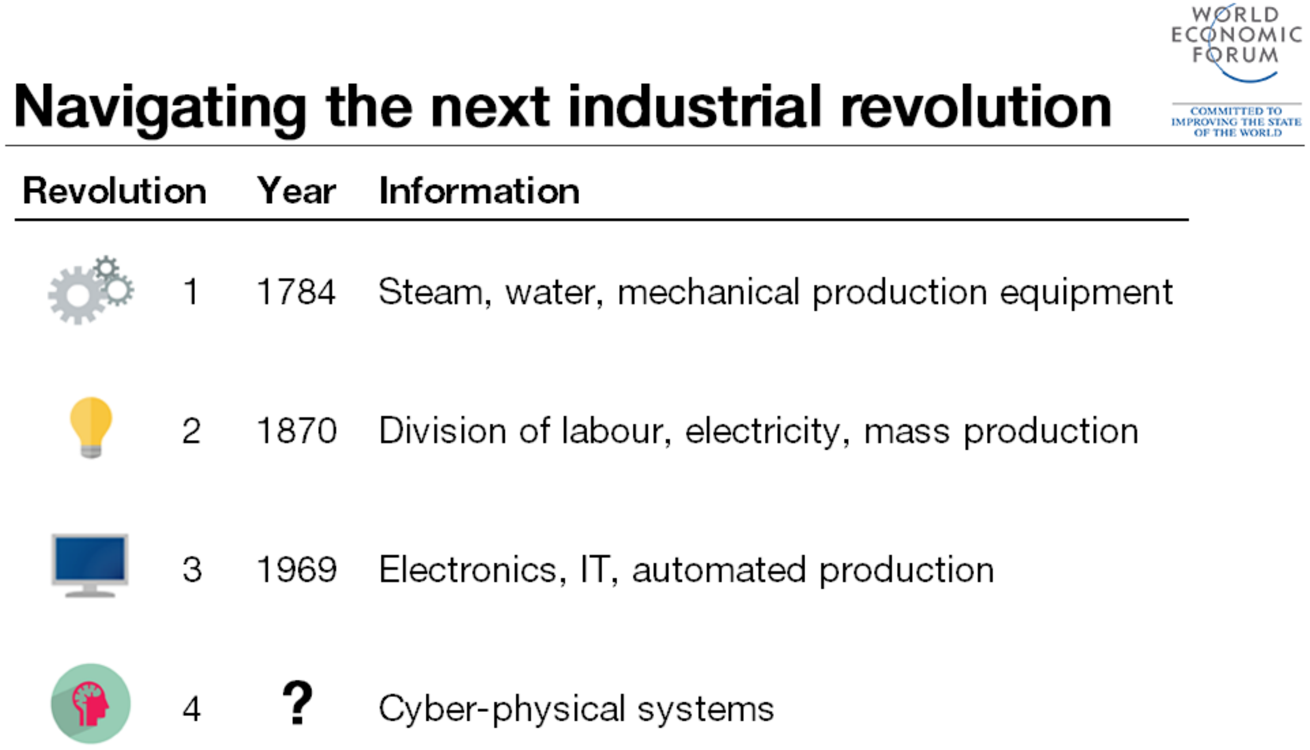
Sincerely,

CEO, X Law Group

CYBERSECURITY ADOPTION CURVES FOR SMBs



THE FOURTH INDUSTRIAL REVOLUTION



WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Navigating the next industrial revolution

Revolution	Year	Information
1	1784	Steam, water, mechanical production equipment
2	1870	Division of labour, electricity, mass production
3	1969	Electronics, IT, automated production
4	?	Cyber-physical systems

We commonly refer to The Fourth Industrial Revolution as, **The Digital Age.** This revolution is powered by cloud, social, mobile, the Internet of things (IoT), artificial intelligence (AI) and machine learning (ML), along with increasing computing power and data.

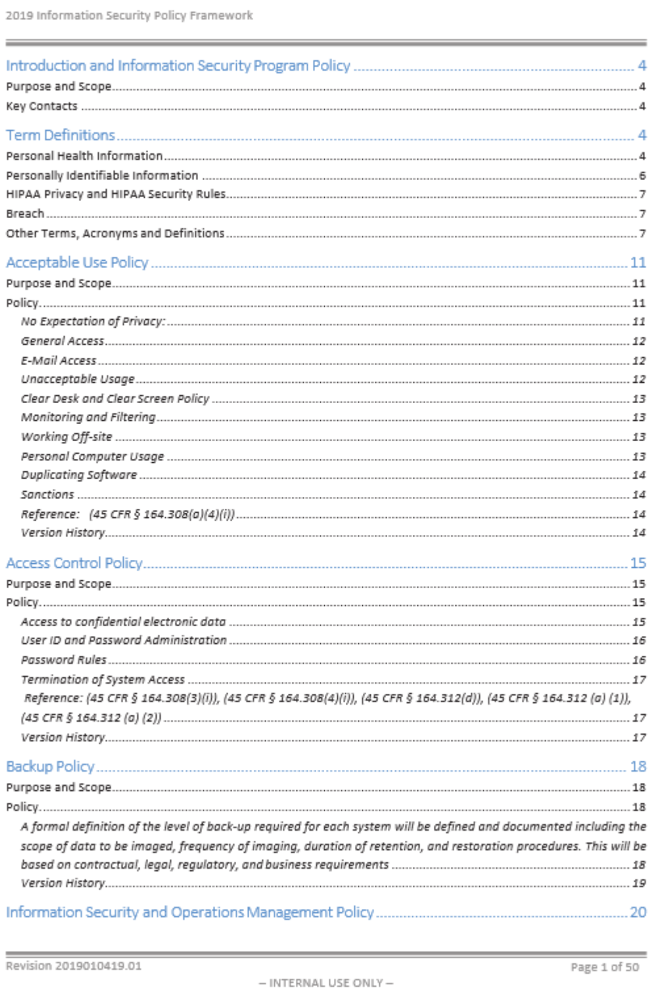
Source: https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/

The Cybersecurity Questionnaire

THE TOP 10 SECURITY QUESTIONS ASKED

1. Do you have an Information Security Policy and how often is it updated?
2. Do you have an Information Security Officer that is qualified for the role?
3. Do you conduct annual Security Risk Assessments?
4. Are you conducting annual vulnerability/penetration testing of your network?
5. Do you have an Access Privileges Policy?
6. Do you have a Third-Party Service Provider Security Policy?
7. Do you perform annual security awareness training with executives and employees?
8. Is your data encrypted in transit and at rest?
9. Can you provide a copy of your Disaster Recovery and Business Continuity Plan?
10. Do you have an Incident Response Plan and is it tested and updated annually?

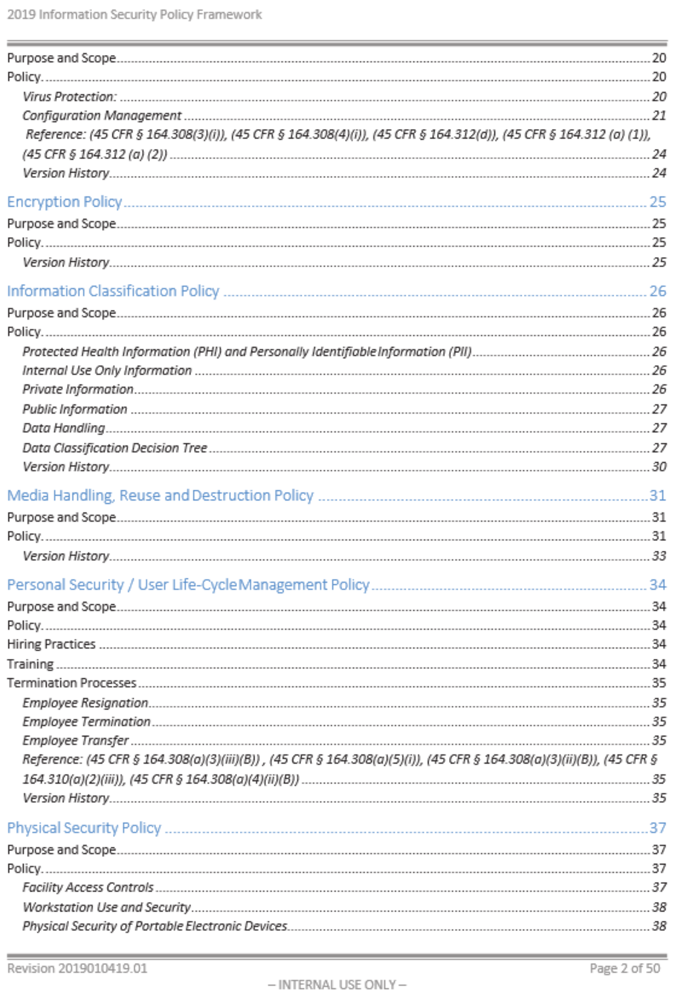
1. Do you have an Information Security Policy and how often is it updated?



2019 Information Security Policy Framework

Revision 2019010419.01 Page 1 of 50

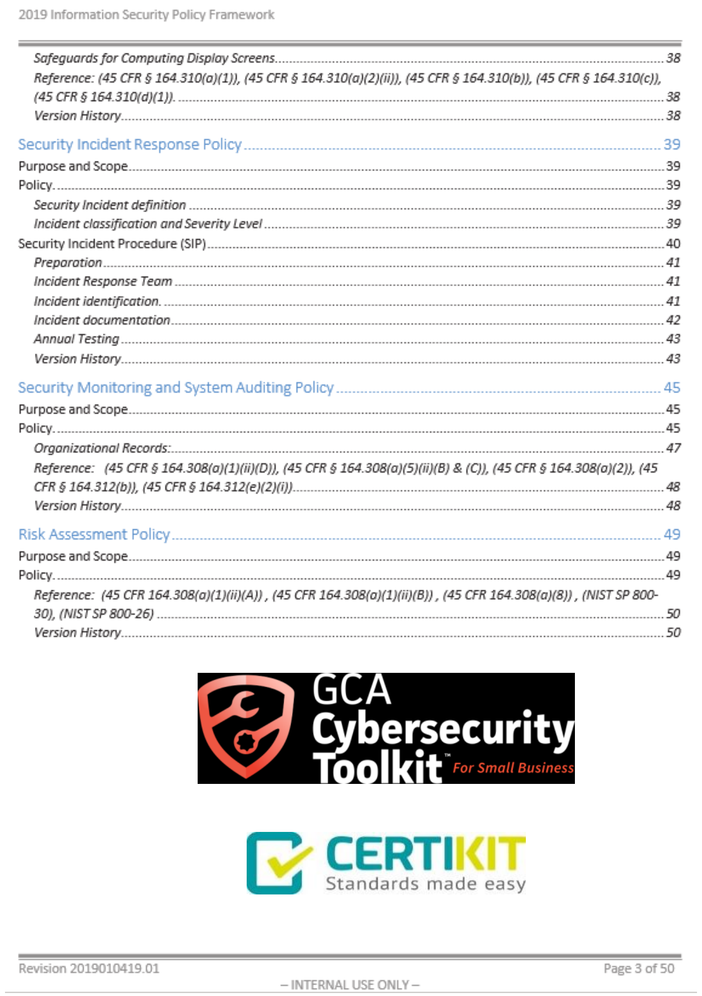
– INTERNAL USE ONLY –



2019 Information Security Policy Framework

Revision 2019010419.01 Page 2 of 50

– INTERNAL USE ONLY –



2019 Information Security Policy Framework

GCA Cybersecurity Toolkit™ For Small Business

CERTIKIT Standards made easy

Revision 2019010419.01 Page 3 of 50

– INTERNAL USE ONLY –

2. Do you have an Information Security Officer that is qualified for the role?

Options:

- Appoint an Internal Resource (preferably in IT) and get them educated
- Hire an Information Security Officer (ISO)
- Outsource to a Security Consulting Firm

3. Do you conduct annual Security Risk Assessments?

Security Risk Assessment Process

1. Classify all sensitive information (electronic and paper)

2. Perform Comprehensive Inventories
- All hardware & software in use or in storage
- All cloud and mobile services
- All partners you do business with

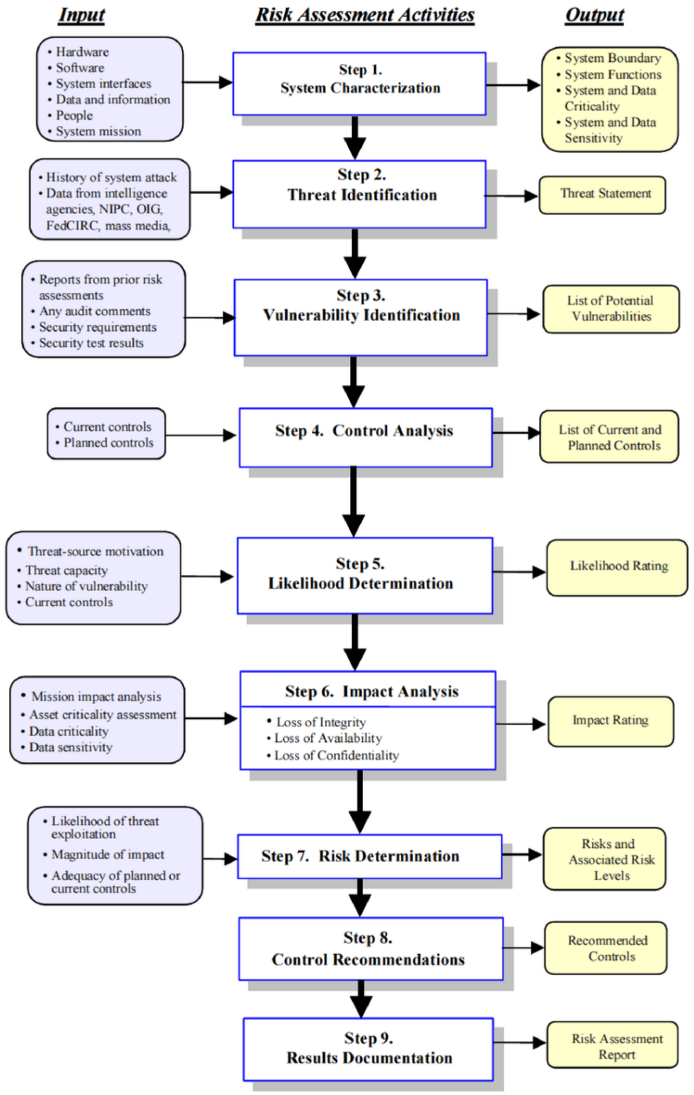
3. "Footprint" your organization's IT infrastructure

4. Assess from the outside-in, and inside-out for best practices
- Think like a hacker!

5. Perform a NIST 800-30 based Qualitative Risk Analysis
- e.g. Likelihood and Impact Determination

6. Decide on security controls to cover your highest areas of risk
7. Schedule the implementation of all controls
8. Repeat as changes are made; formal assessment at least annually!

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Input | Risk Assessment Activities | Output

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Step 1. System Characterization

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

Step 2. Threat Identification

Threat Statement

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Step 3. Vulnerability Identification

List of Potential Vulnerabilities

- Current controls
- Planned controls

Step 4. Control Analysis

List of Current and Planned Controls

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5. Likelihood Determination

Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis
- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Impact Rating

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

Step 8. Control Recommendations

Recommended Controls

Step 9. Results Documentation

Risk Assessment Report

Figure 3-1. Risk Assessment Methodology Flowchart

NIST Based Compliance Frameworks

NIST SP800-53 (rev.5) - provides a catalog of security controls for all U.S. federal information systems except those related to national security.

PCI Security Standards Council™

HIPAA
Health Insurance Portability
& Accountability Act

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

GLBA
Gramm-Leach-Bliley Act

HITRUST
Health Information Trust Alliance

CJIS
Criminal Justice Information Systems

FedRAMP
Federal Risk Authorization Management Program

FEDERAL INFORMATION
~~SECURITY~~ MODERNIZATION
SECURITY MANAGEMENT
ACT OF ~~2002~~ 2014

FFIEC
Federal Financial Institutions Examination Council

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

ALTA 7 PILLARS OF BEST PRACTICES

1. **Licensing -** Establish and maintain current license(s)
2. **Escrow/Trust Accounts** - Adopt and maintain appropriate written procedures and controls
3. **Privacy & Information Security** - Adopt and maintain a written privacy and information security plan
4. **Recording & Pricing Procedures** - Adopt standard real estate settlement policies and procedures that ensure compliance with federal and state consumer financial laws, as applicable.
5. **Title Policy Procedures** - Adopt and maintain written procedures
6. **Professional Liability Insurance** - Maintain appropriate professional liability insurance and fidelity coverage.
7. **Resolving Consumer Complaints** - Adopt and maintain procedures for resolving consumer complaints.

AMERICAN
LAND TITLE
ASSOCIATION

ALTA 7 PILLARS OF BEST PRACTICES

Pillar 3 – Privacy & Information Security

Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information (NPI) as required by local, state and federal laws.

- Physical security of NPI
- Network security of NPI
- Disposal and Maintenance of NPI
- Establish a disaster management plan
- Appropriate management and training of employees to help ensure compliance with information security program
- Oversight of service providers to help ensure compliance with a Company’s information security program
- Audit and oversight procedures to help ensure compliance with Company’s information security program
- Notification of security breaches to customers and law enforcement
- Policies & Procedures

AMERICAN
LAND TITLE
ASSOCIATION

SAMPLE REPORT

Security Risk Assessment

Final Report

Johnson Cardiology

8 May 2016

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

GOLDSKY
CYBER SECURITY SOLUTIONS

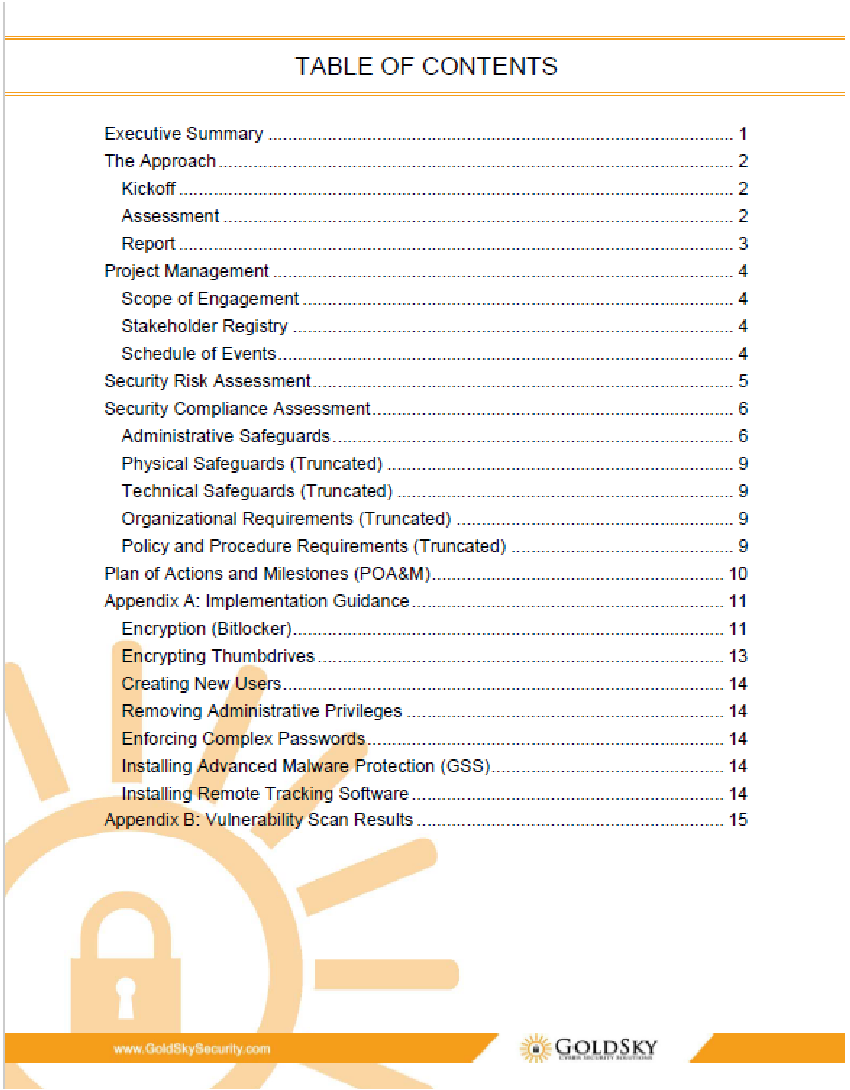


TABLE OF CONTENTS

www.GoldSkySecurity.com GOLDSKY

SAMPLE - RISK ANALYSIS REPORT

Threat Event	Threat Source	Vulnerabilities and Predisposing Conditions	Mitigating Controls Implemented	Likelihood of Event Initiation	Likelihood of Event Succeeds	Overall Likelihood	Level of Impact if Successful	Calculated Risk
Craft (spear) phishing attacks	External Adversarial	(1) Not all employees trained (2) Security awareness training not occurring annually	(1) Anti-Virus Basic deployed on workstations	Very High	High	Very High	Very High	**Very High**
System Breach due to Basic OS Antivirus	External Adversarial Internal Adversarial Internal Non- Adversarial	(1) Vulnerable software on all scanned machines (2) Unpatched Operating Systems (3) No Anti-Phishing (4) No Anti-Malware (5) No Central Management with Alerting (6) No Anti-Ransomware	(1) Anti-Virus Basic deployed on workstations	Very High	Very High	High	Very High	**Very High**
Exploit vulnerabilities on internal organizational information systems	External Adversarial Internal Adversarial	Unpatched Operating Systems	(1) None	Very High	Very High	High	Very High	**Very High**

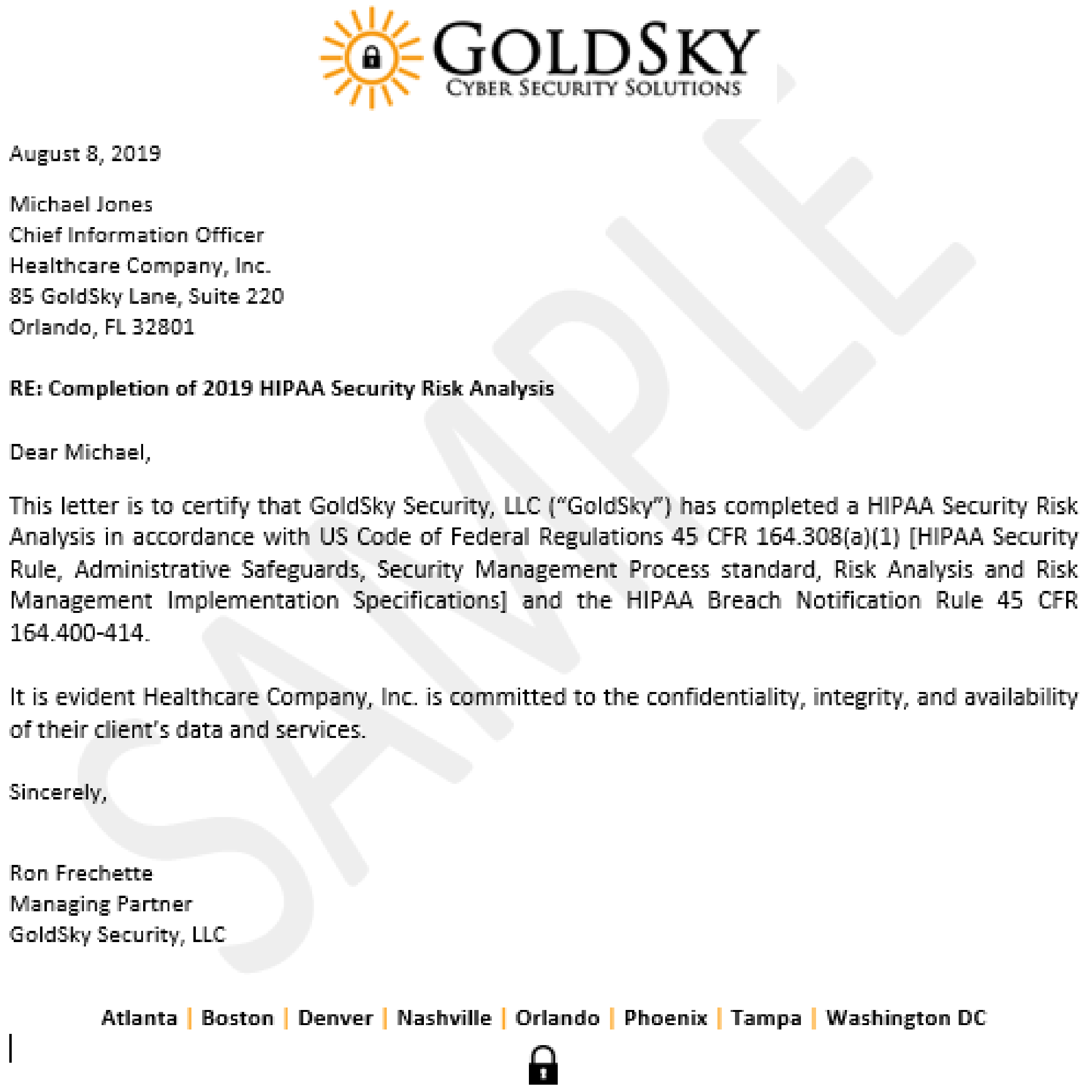
SAMPLE – HIPAA COMPLIANCE GAP ANALYSIS

Key Activity	Established Performance Criteria	Required?	Status	Comments
Conduct Risk Assessment	§164.308(a)(1): Security Management Process §164.308(a)(1)(ii)(a) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Required	Not Compliant	Currently there is no policy in place for conducting an accurate risk analysis. Consider creating and implementing a policy for conducting a risk analysis to review potential risks and vulnerabilities.
Acquire IT Systems and Services	§164.308(a)(1)(i): Security Management Process - Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following: -Applicability of the IT solutions to the intended environment; -The sensitivity of the data; -The organization's security POLICIES, procedures, and standards; and -Other requirements such as resources available for operation, maintenance, and training.	Required	Not Compliant	Currently there is no formal policy in place for Security Management Process Consider creating and implementing a policy to set controls to guard against potential risks and vulnerabilities
Develop and Deploy the Information System Activity Review Process	§164.308(a)(1)(ii)(D): Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Required	Not Compliant	Currently there is no policy in place for monitoring activities such as audit logs and security reports. Consider creating and implementing a policy for monitoring activity. It is assumed that IT is monitoring activity.
Implement a Risk Management Program	§164.308(a)(1): Security Management Process §164.308(a)(1)(ii)(b) - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Required	Not Compliant	Management is aware of lapses in security controls. Consider creating and implementing written policies and procedures.
Select a Security Official To Be Assigned Responsibility for HIPAA Security	§164.308(a)(2): Assigned Security Responsibility - the responsibility for security should be assigned to a specific individual or organization to provide an organization focus and importance to security, and that the assignment be documented.	Required	Not Compliant	Currently the responsibilities of "Security" are on an ad hoc basis by IT and a few department heads. A Security Officer should be assigned.
Assign and Document the Individual's Responsibility	§164.308(a)(2): Assigned Security Responsibility - the responsibility for security should be assigned to a specific individual or organization to provide an organization focus and importance to security, and that the assignment be documented.	Required	Not Compliant	Currently there are no defined duties to implement or monitor security controls. Consider creating a Security Officer's duties and responsibilities

SAMPLE - REMEDIATION ROADMAP

Immediate Goals	Short-Range Goals	Mid-Range Goals
The following activities should be addressed within the next 30 days: 1. Address all medium (and high) vulnerabilities in the attached vulnerability scan results; most of which are update and upgrade related 2. Setup Azure Active Directory or a local Microsoft Active Directory System for central user credential management. 3. Install Central Anti-Virus, Anti-Phishing, Anti-Malware software. IE (Panda Adaptive Defense 360)	The following activities should be addressed within the next 90 days: 1. Expand a centralized logging capability with security analysis abilities. 2. Adopt, and implement all recommended plans, policies, and procedures. 3. Implement Cyber Security Training Program for all employees. 4. Implement Backup of all Data Cloud and local where it applies after contract reviews.	The following activities should be addressed within the next 9 months: Begin performing routine internal vulnerability management. For scanning, we recommend Tenable Nessus. This service can be provided by a Managed Security Service Provider (MSSP) 1. Implement a helpdesk system reports for tracking top monthly issues. 2. Perform Top 10 Helpdesk Issue reviews to determine problem heatmap exercise to address remedy's to lower support requests where possible.

SAMPLE – SRA Letter of Completion



GOLDSKY
CYBER SECURITY SOLUTIONS

August 8, 2019

Michael Jones
Chief Information Officer
Healthcare Company, Inc.
85 GoldSky Lane, Suite 220
Orlando, FL 32801

RE: Completion of 2019 HIPAA Security Risk Analysis

Dear Michael,

This letter is to certify that GoldSky Security, LLC ("GoldSky") has completed a HIPAA Security Risk Analysis in accordance with US Code of Federal Regulations 45 CFR 164.308(a)(1) [HIPAA Security Rule, Administrative Safeguards, Security Management Process standard, Risk Analysis and Risk Management Implementation Specifications] and the HIPAA Breach Notification Rule 45 CFR 164.400-414.

It is evident Healthcare Company, Inc. is committed to the confidentiality, integrity, and availability of their client's data and services.

Sincerely,

Ron Frechette
Managing Partner
GoldSky Security, LLC

Atlanta | Boston | Denver | Nashville | Orlando | Phoenix | Tampa | Washington DC

HOW INSURANCE COMPANIES RATE TITLE COMPANIES

Insurance companies look at three specific matters when rating title companies' and law firms' premiums for crime policies:

1. Volume of data the firm handles
2. The firm's policies and procedures
3. How well the firm trains its staff

So, the idea that law offices protect themselves through training and procedures is not only an ALTA Best Practice but is something that drives insurance premium.

4. Are you conducting annual vulnerability/penetration testing of your network?

Searching for known vulnerabilities:

- Does NOT actively try to exploit a client
- Is NOT penetration testing or ethical hacking
- Internal and/or External in scope

Process:

- Discover targets through interviews and scans
- Perform automated vulnerability scans
- Analyze the results

OpenVAS
Open Vulnerability Assessment System

Nessus® vulnerability scanner

nexpose®

Summary of Findings:

Assets Tested	Scan Profile	Finding Summary			
		Low	Med	High	Critical
Orlando, FL	Authenticated	142	421	68	15
Percentage of Total Events		**26 %**	**59 %**	**12 %**	**2 %**

5. Do you have an Access Control Policy?

General principles when designing an access control policy:

- ***Defense in Depth*** – security must not depend upon any single control but be the sum of a number of complementary controls
- ***Least Privilege*** – the default approach taken must be to assume that access is not required, rather than to assume that it is
- ***Need to Know*** – access is only granted to the information required to perform a role, and no more
- ***Need to Use*** – Users will only be able to access physical and logical facilities required for their role

GCA Cybersecurity Toolkit™ For Small Business

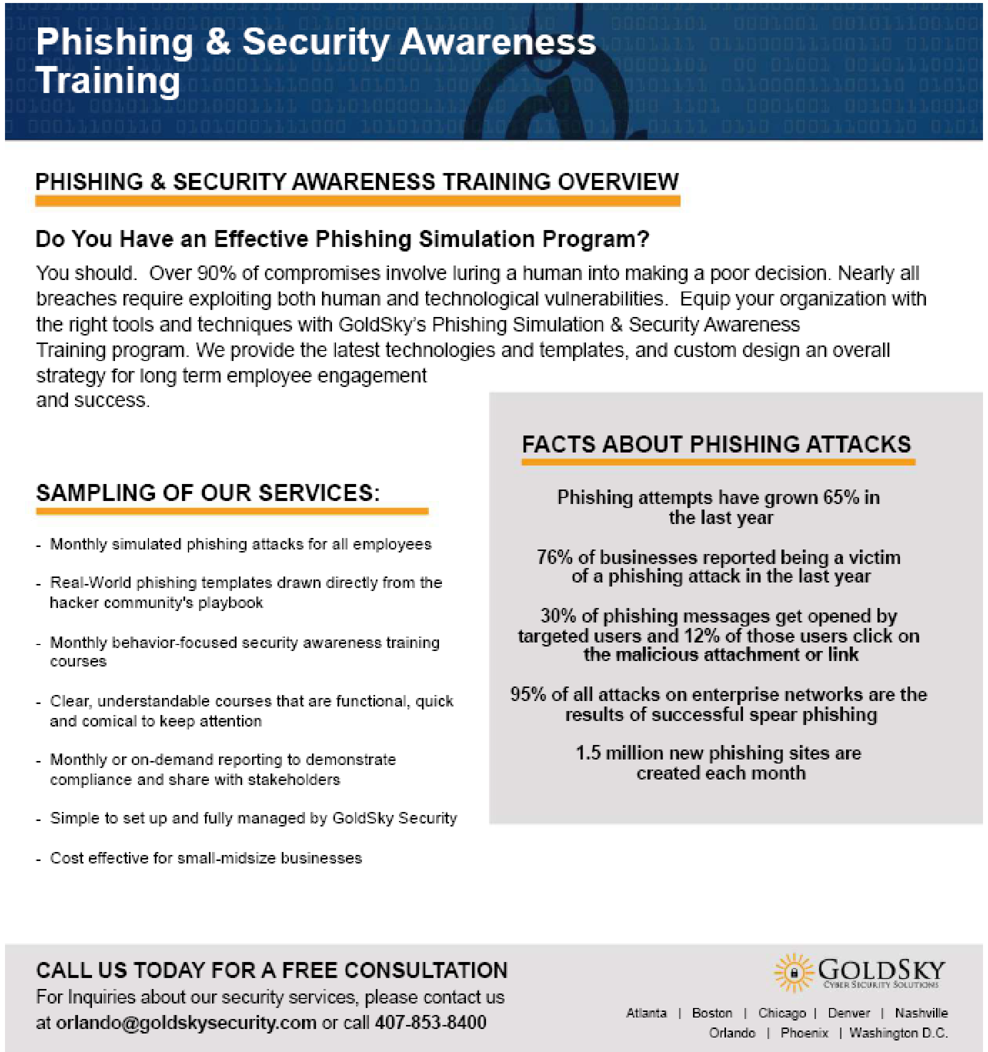
CERTIKIT Standards made easy

6. Do you have a Third-Party Service Provider Security Policy?

Framework for a Third-Party Management Program

- **Develop the Plan –** Assign a person to spearhead the project and define clear roles and responsibilities for those within your organization who will write the policy, obtain proper documentation from vendors, monitor vendor/partner performance, etc.
- **Build a Due Diligence Process –** Determine which vendor/partners are audited or assessed by outside auditing firms and willing to share results.
- **Have a Reporting System –** Identify reports that you should be receiving from vendors to monitor their performance on a periodic basis. (ISO, SOC, Penetration Tests, etc.)
- **Continuous Monitoring –** Set up an ongoing monitoring process to make sure that the vendor continues to meet expectations. May depend on client requirements.
- **Access to Sensitive Data –** Consider what types of data is accessible by your third-parties, what types of transactions they perform, etc., to determine the risk associated with each vendor.
- **Termination Process –** Have a formal process in place that defines exactly what you would do if you find it necessary to terminate your relationship with a vendor/partner or if the vendor terminated their relationship with your organization.

7. Do you perform annual security awareness training with executives and employees?



Phishing & Security Awareness Training

PHISHING & SECURITY AWARENESS TRAINING OVERVIEW

Do You Have an Effective Phishing Simulation Program?

You should. Over 90% of compromises involve luring a human into making a poor decision. Nearly all breaches require exploiting both human and technological vulnerabilities. Equip your organization with the right tools and techniques with GoldSky's Phishing Simulation & Security Awareness Training program. We provide the latest technologies and templates, and custom design an overall strategy for long term employee engagement and success.

SAMPLING OF OUR SERVICES:

- Monthly simulated phishing attacks for all employees
- Real-World phishing templates drawn directly from the hacker community's playbook
- Monthly behavior-focused security awareness training courses
- Clear, understandable courses that are functional, quick and comical to keep attention
- Monthly or on-demand reporting to demonstrate compliance and share with stakeholders
- Simple to set up and fully managed by GoldSky Security
- Cost effective for small-midsize businesses

FACTS ABOUT PHISHING ATTACKS

Phishing attempts have grown 65% in the last year

76% of businesses reported being a victim of a phishing attack in the last year

30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link

95% of all attacks on enterprise networks are the results of successful spear phishing

1.5 million new phishing sites are created each month

CALL US TODAY FOR A FREE CONSULTATION

For Inquiries about our security services, please contact us at orlando@goldskysecurity.com or call 407-853-8400

GOLDSKY
Cyber Security Solutions

Atlanta | Boston | Chicago | Denver | Nashville
Orlando | Phoenix | Washington D.C.

8. Is your data encrypted in transit and at rest?

What is email encryption?

- Email encryption relies on a Public Key Infrastructure or PKI, in most cases, a combination of a private key (known only by you) and a public key (known only to those you choose to distribute it to or even made publicly available).

Why is this important for law firms?

- Minimizes risk of data theft or leakage for clients and the practice.
- Encrypting email messages before they’re sent means that even if a hacker or anyone other than the intended recipient should intercept your email messages, they’re unreadable, and essentially useless.

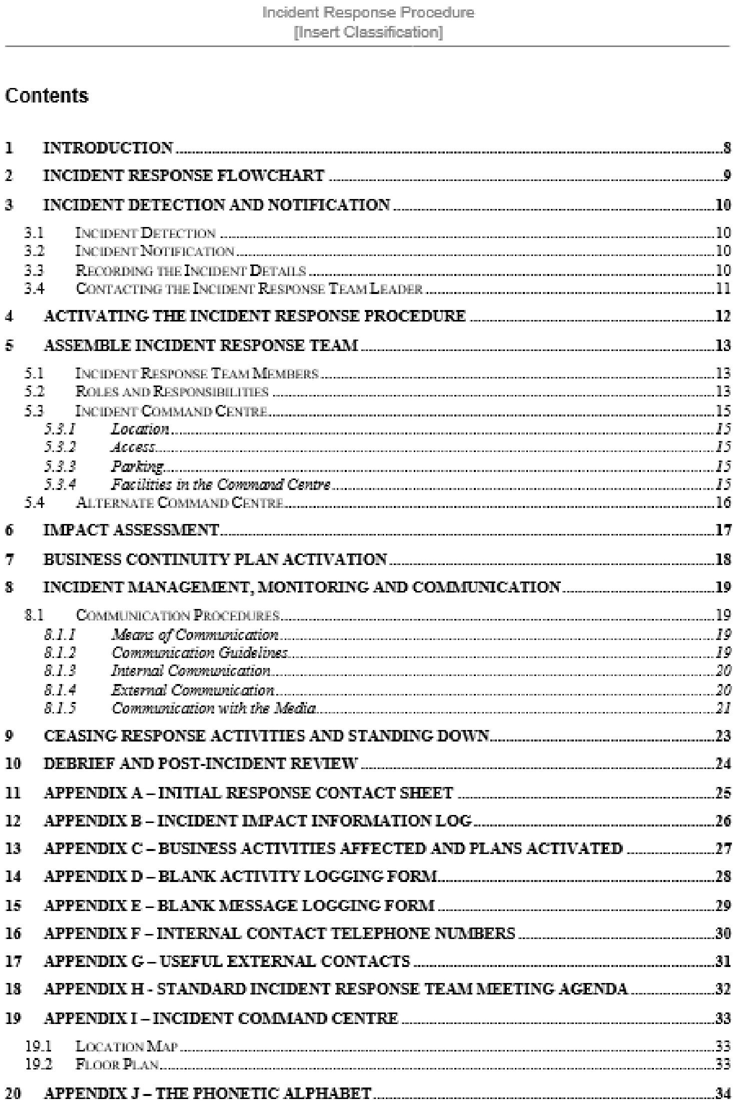
What is the best type of email encryption solution?

- Impenetrable email protection
- The one with the least amount of clicks to send emails
- Easiest to implement for both the sender and receiver
- It can be tracked once sent (who opened and when)
- Postmarks confidential information and is a *federally-approved form of legal delivery* so you can send all your certified documents, securely and instantaneously

EMAIL ENCRYPTION FEATURES

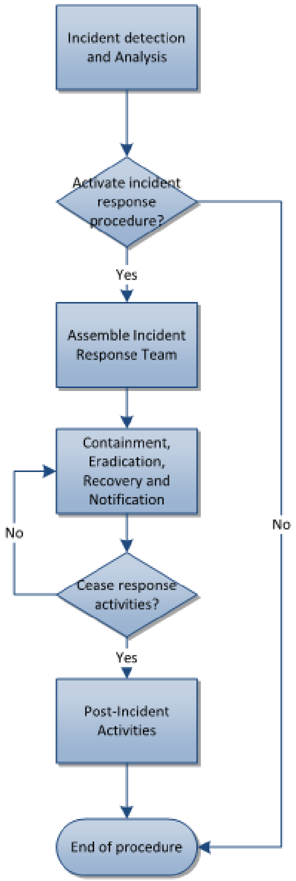
- Military-Grade Encryption
- One-Click Encryption
- Email Tracking
- Postmark Certified Delivery
- Data Sensitivity Auto Detection
- Mobile Secure

9. Can you provide a copy of your Incident Response and Business Continuity Plan?

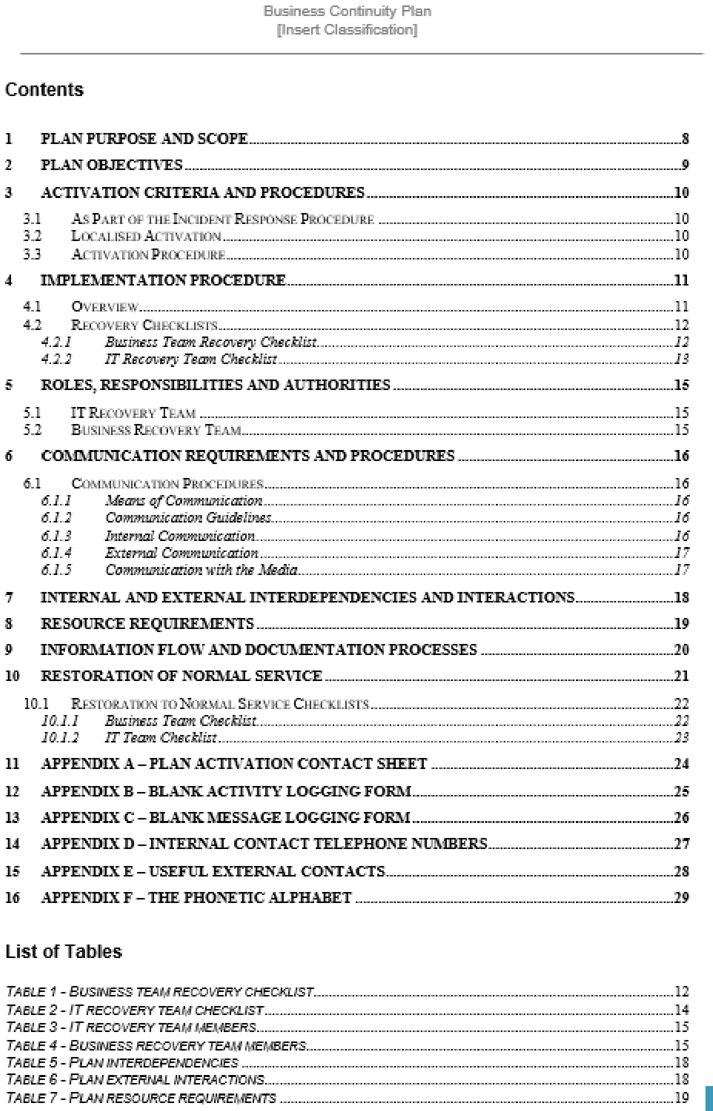


Incident Response Procedure
[Insert Classification]

Contents



Incident detection and Analysis
Activate incident response procedure?
Yes
No
Assemble Incident Response Team
Containment, Eradication, Recovery and Notification
No
Cease response activities?
Yes
Post-Incident Activities
End of procedure

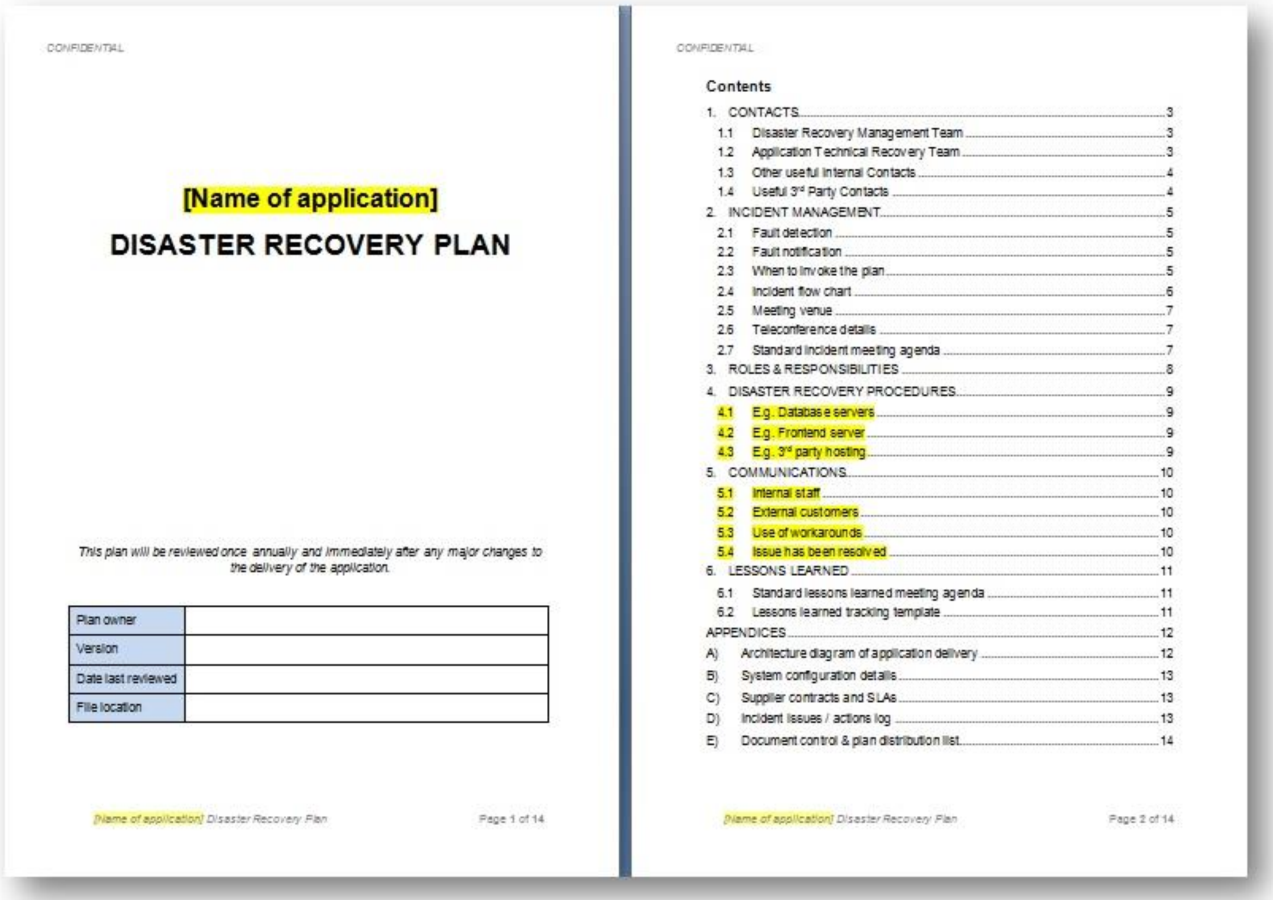


Business Continuity Plan
[Insert Classification]

Contents

List of Tables

10. Do you have a Disaster Recovery Plan and is it tested and updated annually?



CONFIDENTIAL

[Name of application]

DISASTER RECOVERY PLAN

This plan will be reviewed once annually and immediately after any major changes to the delivery of the application.

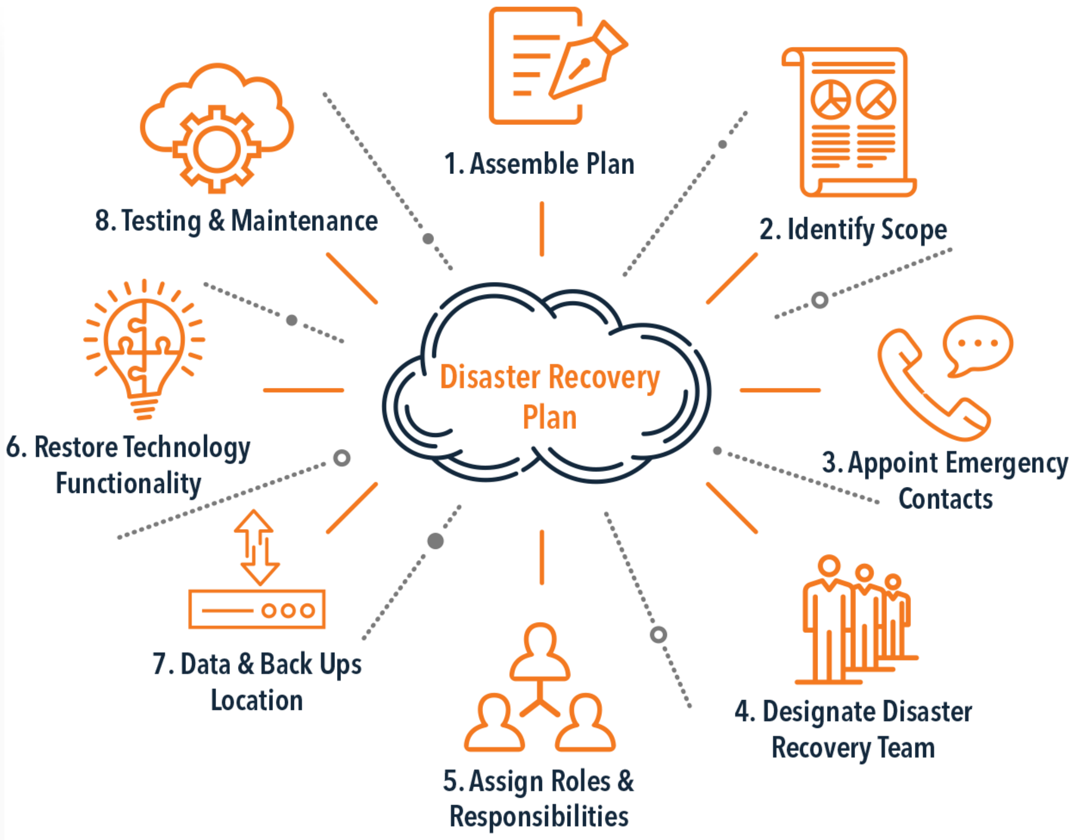
Plan owner	
Version	
Date last reviewed	
File location	

[Name of application] Disaster Recovery Plan Page 1 of 14

CONFIDENTIAL

Contents

[Name of application] Disaster Recovery Plan Page 2 of 14


Disaster Recovery Plan
1. Assemble Plan
2. Identify Scope
3. Appoint Emergency Contacts
4. Designate Disaster Recovery Team
5. Assign Roles & Responsibilities
6. Restore Technology Functionality
7. Data & Back Ups Location
8. Testing & Maintenance

GCA Cybersecurity Toolkit For Small Business

CERTIKIT Standards made easy

ETHICAL CONCERNS… PRACTICING DUE-CARE

You are a custodian of sensitive data:

- Financial Records
- Medical Records (HIPAA)
- Private and (potentially) damaging information
- Credit Card Information (PCI)

Attorneys' Duty to Safeguard Information

- The ABA ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to clients (ABA Model Rules 1.1 and 1.6 and Comments).
- Attorneys also have common law duties to protect client information and often have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information, like health and financial information.

Due Care

- Have you taken reasonable measures to secure client data?
- Are you aware of all your legal and regulatory obligations?
- Do you know your own vulnerabilities?
- Are you aware of the threats to the security of your data?

Source: American Bar Association

Florida State Law – What is FIPA?

Florida Information Protection Act of 2014, Sec. 501.171, F.S. is a Florida state law governing privacy rules for entities handling personal information.

Who is Covered Under FIPA? - a Covered Entity is defined as a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. This also can include a government entity.

FIPA protects personal information (which means any of the following):

- Names, Social Security number, driver's license or identification card number, passport number, military identification number
- Financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- A username or email address, in combination with a password or security question and answer that would permit access to an online account.
- Customer Records include any material, regardless of physical form, on which personal information is recorded or preserved – including written or spoken words, graphics, or print.

FIPA is a Florida state law with broad enforcement – includes companies doing business in Florida, and those with clients in Florida are responsible for complying with FIPA requirements.

What Can I Do to Ensure My Company is Complying with FIPA Requirements?
The first steps in compliance with FIPA requirements are performance of a risk assessment and education.

TOP THREATS TO THE REAL ESTATE INDUSTRY

Unlike most industries, there is no federal law requiring real estate businesses to implement information security programs. That has led to real estate businesses having vulnerable systems.

Business email compromise - A business email compromise **(BEC)** is an attack that deceptively convinces businesses to wire funds to criminal back accounts by pretending to be business counterparties, such as vendors or real estate sellers.

Ransomware – Ransomware is a form of malware that encrypts data on computers and makes the data unavailable until a ransom is paid, has become an immensely profitable method for hackers to attack businesses.

Other Malware - Banking Trojans are used by criminals to capture a victim's banking credentials to wipe the bank account clean and gain access to PII.

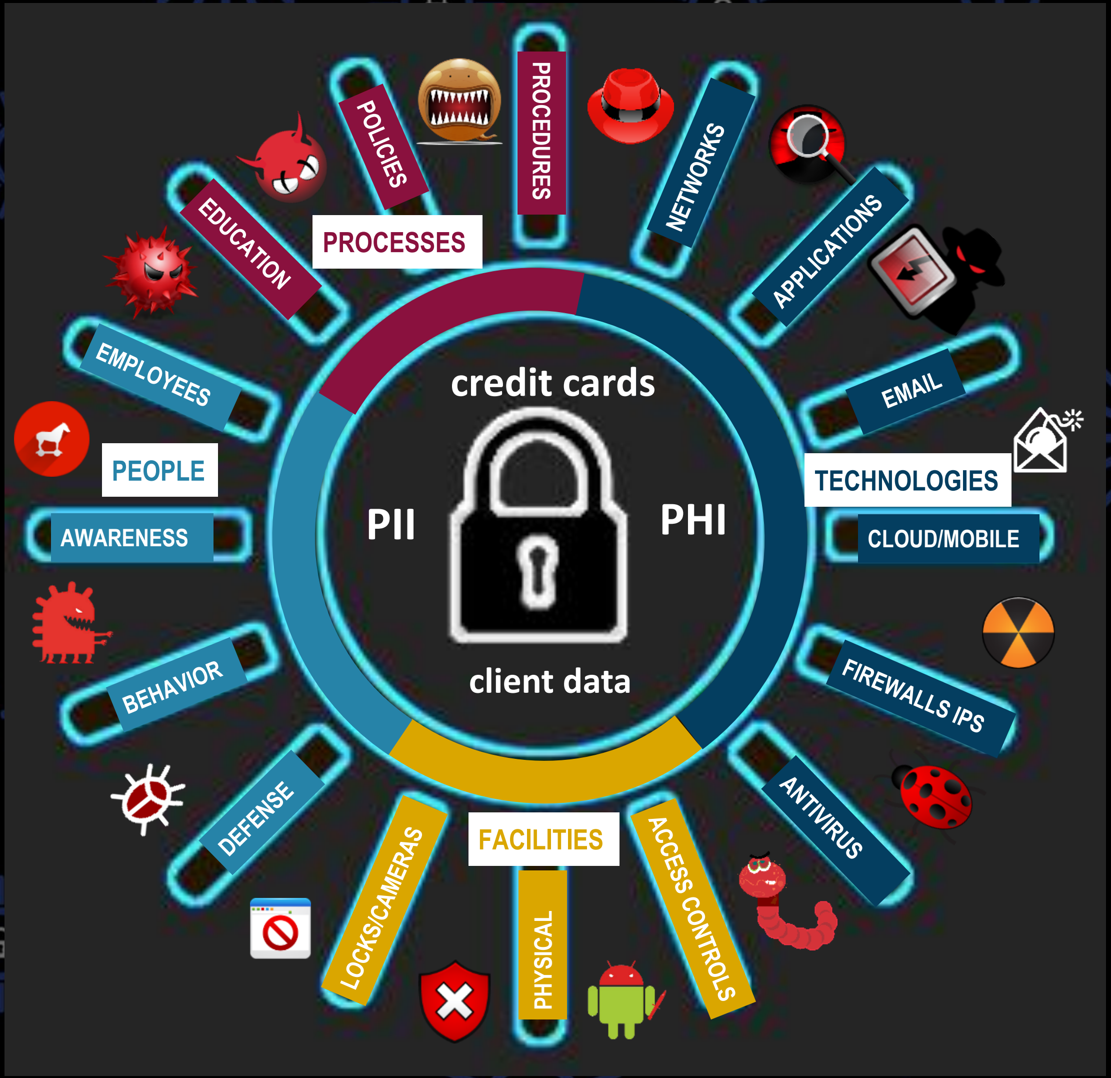
Originally designed as a banking Trojan, Emotet has evolved over the years into malicious code capable of delivering a large-scale botnet capable of targeting a number of systems and considered to be one of the deadliest malware families operating in the wild, security experts say.

Third-Party Vendors - A criminal does not need to hack a business to get that business's sensitive data these days: it can target trusted vendors like cloud providers that store other parties' sensitive information.

Adopting a Cybersecurity Framework

Your Digital Footprint

Four threat vectors around a digital footprint:



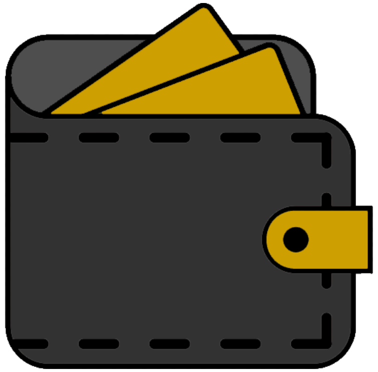
How secure is your digital footprint?

PRIMARY OBJECTIVES FOR BUILDING A SECURITY PROGRAM

Primary Objectives

Avoid Compromise
Costs and Brand Damage

Achieve Compliance
Follow the Law and Avoid Fines



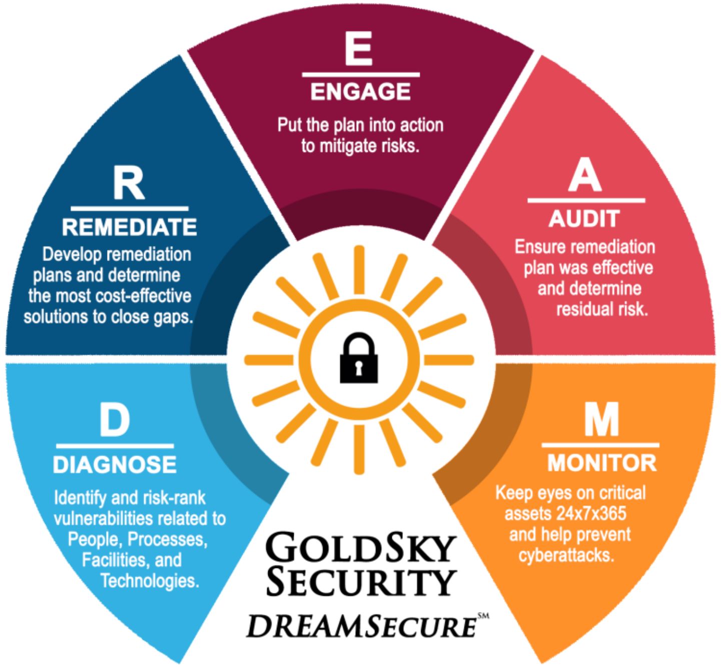
Affordable Solutions
Custom Designed for SMBs

WHAT’S THE RIGHT APPROACH?

The Right Approach

Evaluate, Identify, and Manage Risk

DREAMSecure℠ CYBER RISK MANAGEMENT SYSTEM



E
ENGAGE
Put the plan into action to mitigate risks.
A
AUDIT
Ensure remediation plan was effective and determine residual risk.
M
MONITOR
Keep eyes on critical assets 24x7x365 and help prevent cyberattacks.
D
DIAGNOSE
Identify and risk-rank vulnerabilities related to People, Processes, Facilities, and Technologies.
R
REMEDIATE
Develop remediation plans and determine the most cost-effective solutions to close gaps.
GOLDSKY SECURITY
DREAMSECURE℠

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Key Benefits:

- Easy to Understand, Easy to Implement
- Reduces Risks of Data Theft and Cyber Breaches
- Reduces Risks of Fines, Penalties and Lawsuits for Non-Compliance
- Affordable for Small-Midsize Businesses

It's a journey, not a destination.

SELF-ASSESSMENT RESOURCES

GCA Cybersecurity Toolkit™ For Small Business

https://gcatoolkit.org/smallbusiness/

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

https://www.nist.gov/cyberframework/general-resources

CIS® Center for Internet Security®

https://www.cisecurity.org/

AND REMEMBER …

PASSWORDS ARE LIKE
UNDERPANTS
Change them often, keep them private and never share them with anyone.

THANK YOU FOR YOUR TIME TODAY!

QUESTIONS?