



Caught in The Dark Web – A Real Estate Attorney's View

Ron Frechette

Founder and CEO, Goldsky Security

Christopher Dix

Shareholder, Smith, Hulsey & Busey



Presenters



Ron Frechette, CEO

GoldSky Security, LLC

Ron is a cybersecurity and IT staffing entrepreneur who since 2010 has dedicated his career to helping companies reduce the risks of cyber attacks, malware threats, and data theft.

He has a strong knowledge base in all aspects of IT security and compliance to include: FedRAMP, FISMA, GDPR, GLBA, HIPAA/HITECH, HITRUST, ISO 27001/02, NIST CSF, NIST 800-53, PCI-DSS, and SSAE 18 (SOC 1, SOC 2).

Ron is an avid writer and blogger who studies emerging cybersecurity trends and shares his knowledge through local publications such as The Park Press and Orlando Medical News.

Contact Info:

<https://goldskysecurity.com/staff/ronald-frechette/>
ron.frechette@goldskysecurity.com

Direct: (321) 325-2073



Christopher Dix, CPA, JD

Smith, Hulsey & Busey

Chris Dix is a technology-focused attorney and CPA with experience litigating business disputes, healthcare regulatory matters, bankruptcy and sports corruption arbitrations. He also advises clients regarding e-discovery, cybersecurity, data breaches (including HIPAA security and privacy issues), social media and other forms of electronic evidence.

Chris obtained a Bachelor of Science in Accounting, with honors, and a Master of Accounting from the University of Florida. Chris also obtained a Juris Doctorate, with honors, from the University of Florida College of Law.

Chris is a licensed CPA in Florida. He has also earned the CEDS designation from ACEDS, and was co-founder and President of the organization's local chapter, ACEDS Jacksonville.

Contact Info:

<https://www.linkedin.com/in/chrisdix1/>
cdix@smithhulsey.com

Direct: (904) 359-7730



Overview

- The World Wide Web and the Dark Net
- What is Tor
- How Tor Works
- Live Dark Net Demo
- The Threat Actors
- Ethical Concerns
- Federal and State Compliance Laws
- Primary Objectives to Mitigate Risk
- A Cyber Risk Management System
- Security Tips - How to Mitigate Your Risk



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 number 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

CONFIDENTIAL AND PROPRIETARY



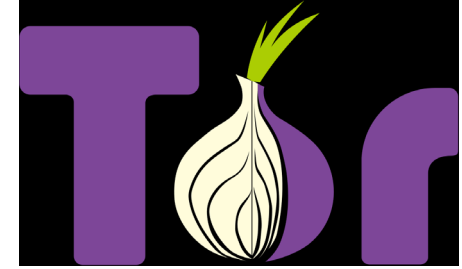


The World Wide Web





What is Tor?



- Tor is a service that helps you to protect your anonymity while using the Internet.
- Developed in the mid-1990s by United States Naval Research Laboratory to protect US intelligence communications online.
- Further developed by Defense Advanced Research Projects Agency (DARPA).
- Tor is comprised of two parts:
 1. Software you can download that allows you to use the Internet anonymously,
 2. a volunteer network of computers that makes it possible for that software to work.





How Tor Works

How Tor Works

Alice



Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



Jane



Bob



Tor node



unencrypted link




encrypted link

- Encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe.
- These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location







Live Tor Demo

About Tor


 Tor Browser

Search or enter address

  Search


Tor Browser
7.5.3



Welcome to Tor Browser

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)



Search securely with [DuckDuckGo](#).

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

- [Tips On Staying Anonymous »](#)
- [Tor Browser User Manual »](#)

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

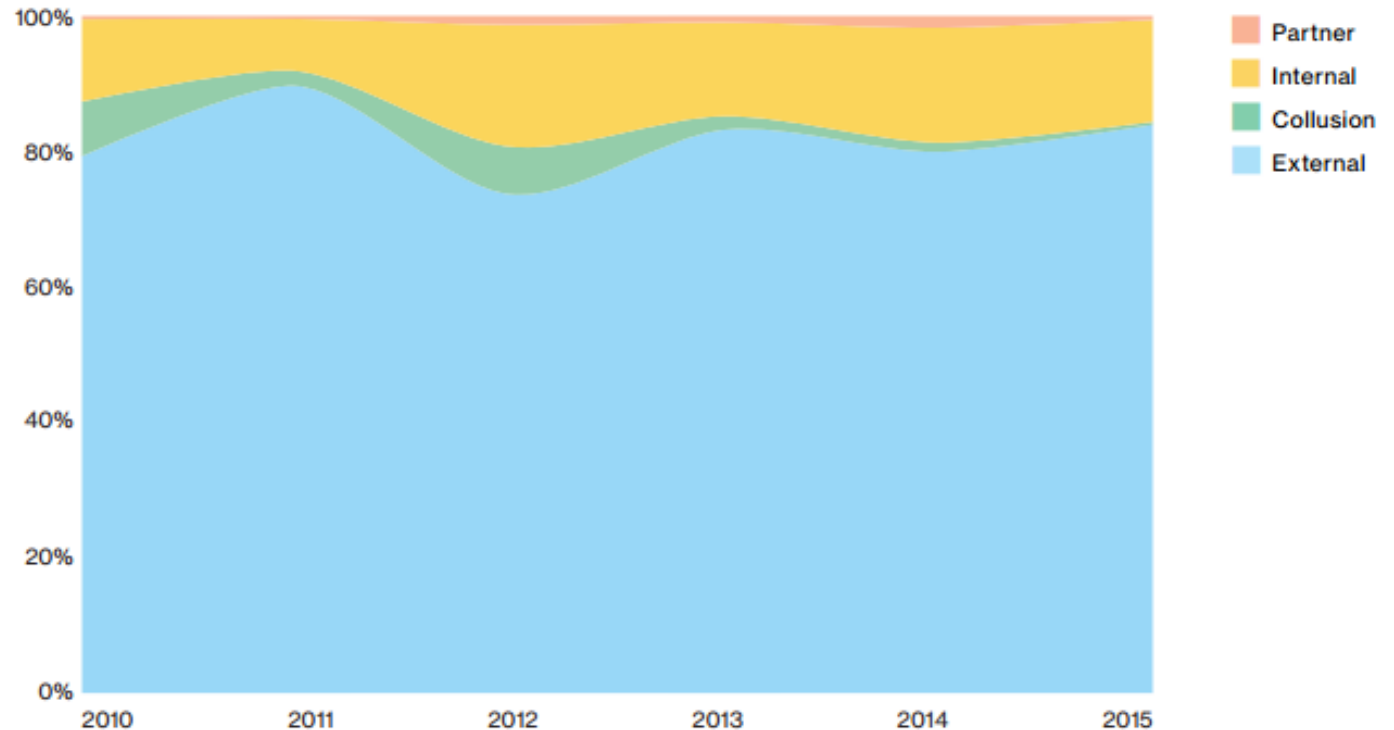
- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)



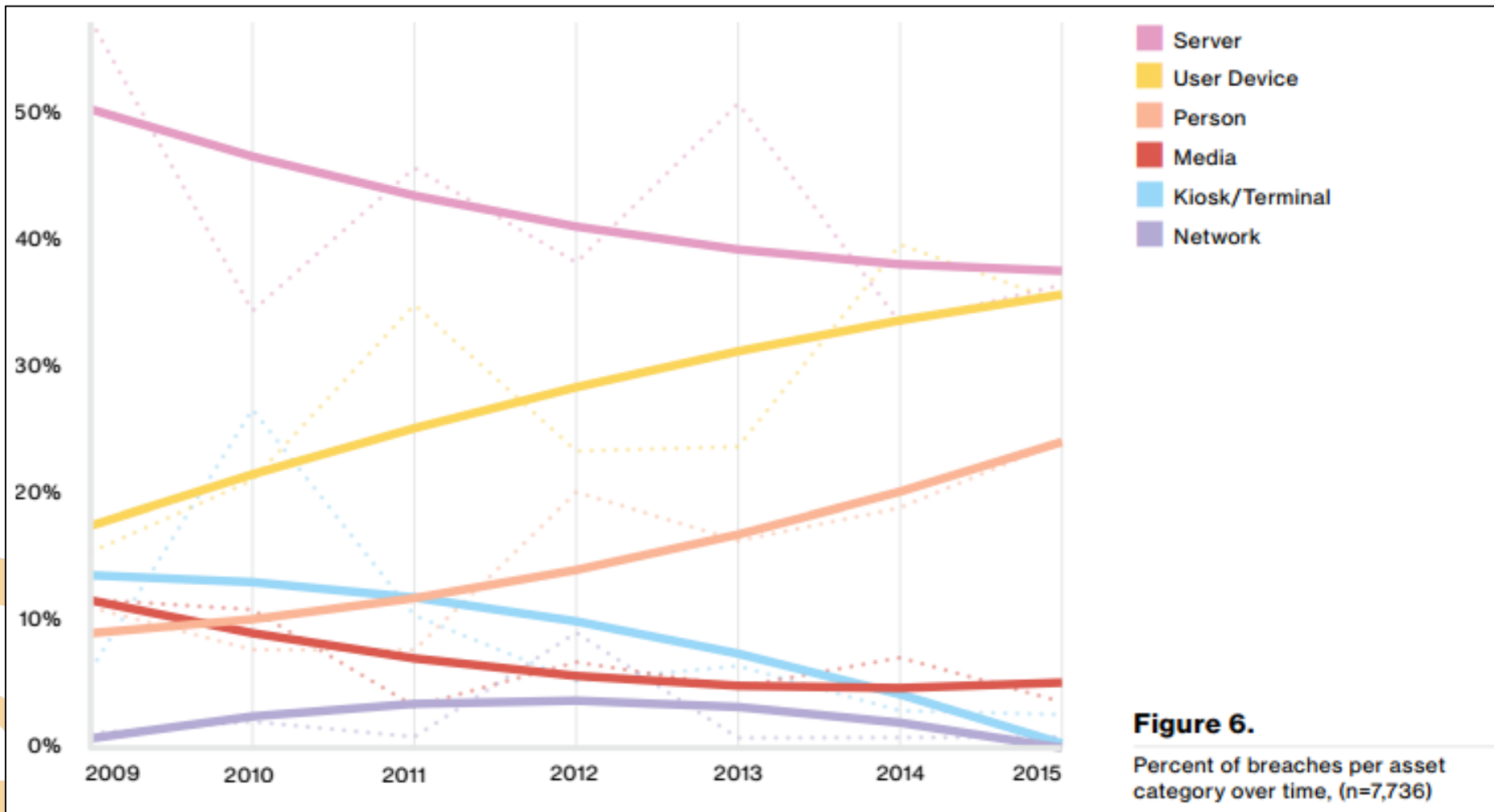
Who are the attackers?

- **Organized Crime Organizations**
 - Large syndicates of attackers
 - Hierarchical organizations; Mafia
- **State-Sponsored Attackers**
 - Government organizations
 - Russia, China, Iran, North Korea, etc...
- **Script Kiddies**
 - Use downloaded tools and scripts
 - Motivated by fame
- **Other Professionals**
 - Usually experimenting, learning, or shaming
- **Hacktivists**
 - All-the-above
 - Motivated by a social cause





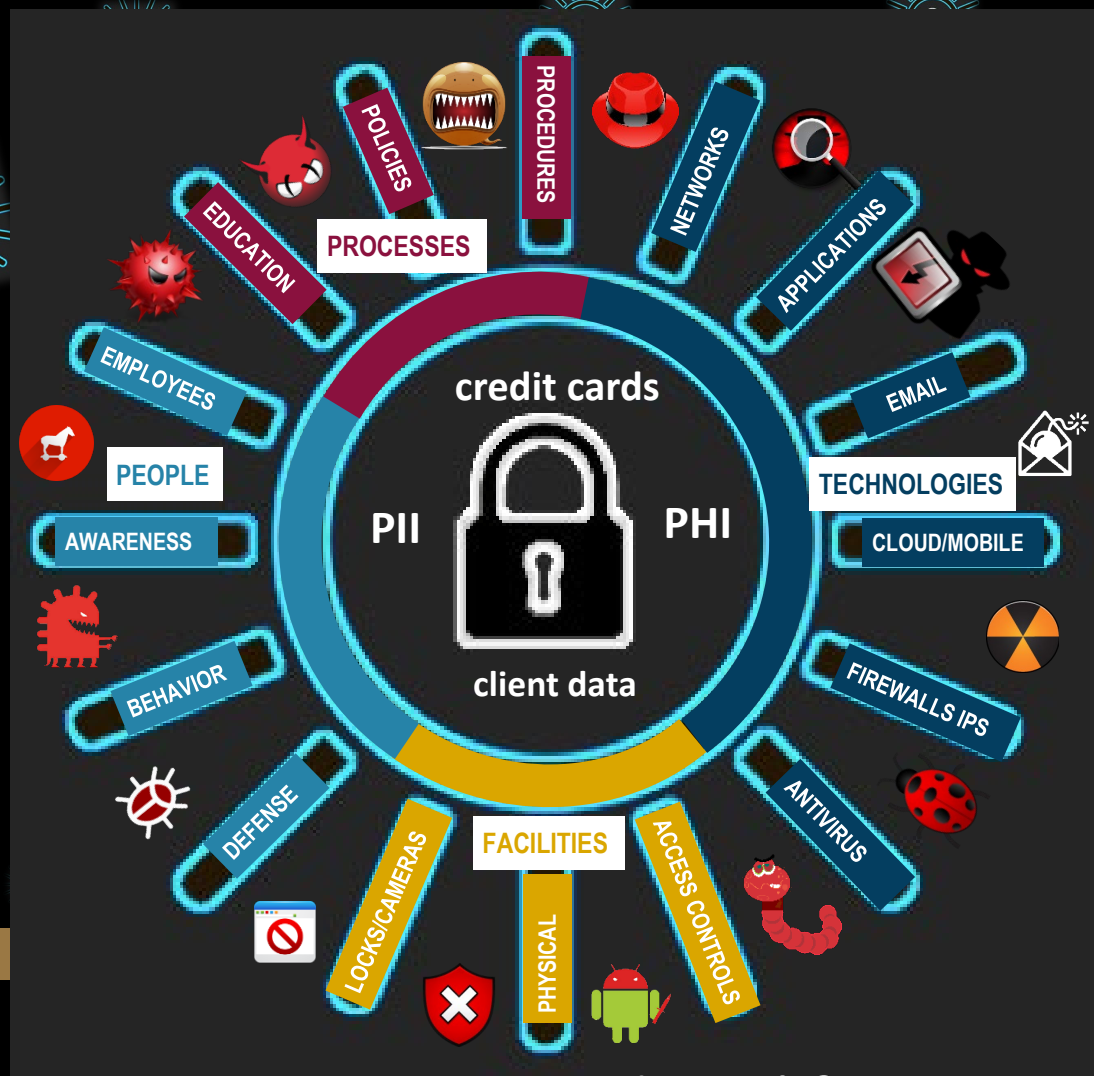
What are they attacking?





Digital Footprints in Cyber Space...

Four threat vectors around a digital footprint:



How secure is your digital footprint?



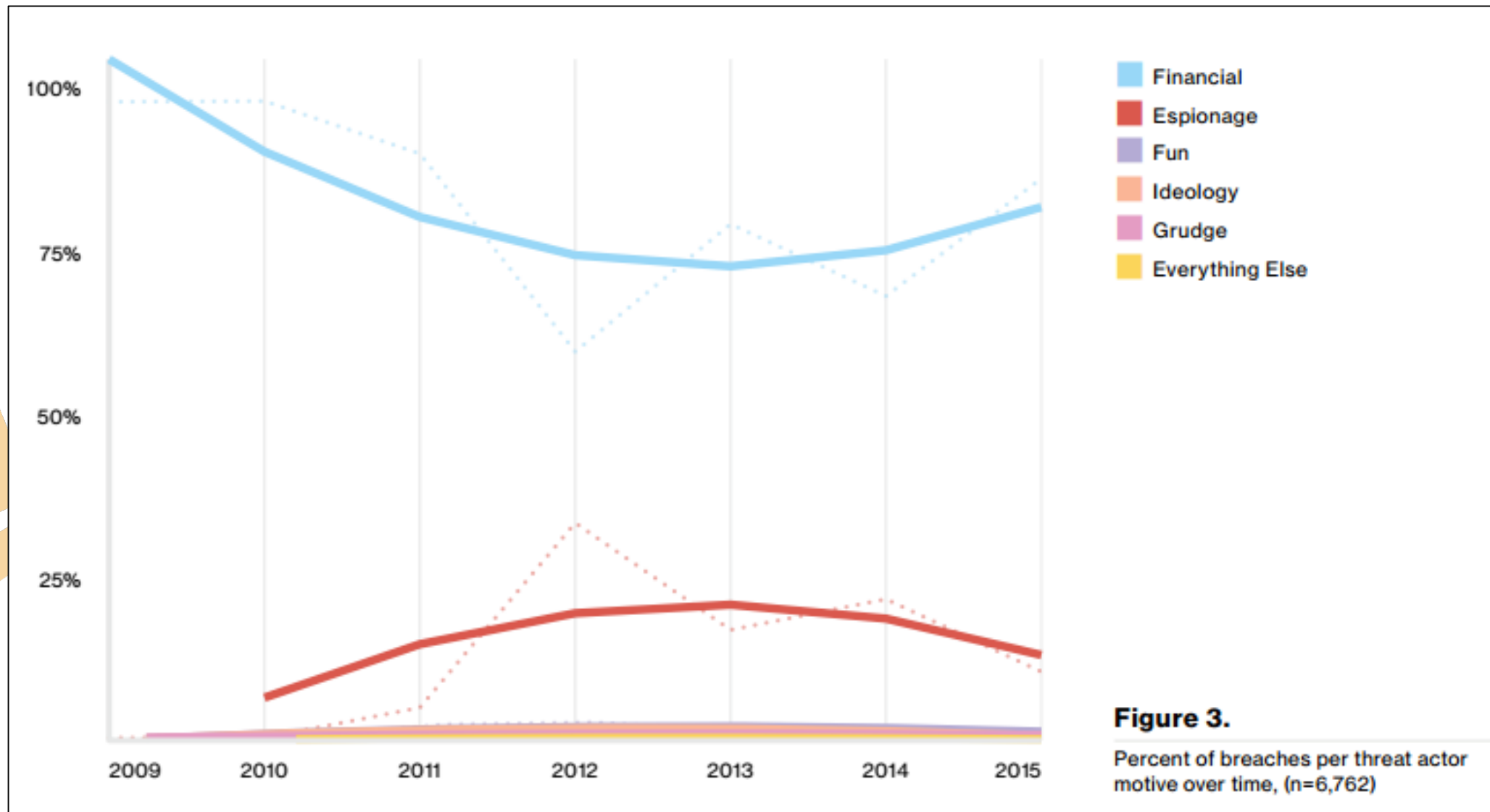


How are they attacking?





Hacker Motives





Hackers are selling access to law firm secrets on dark web sites...



- Law firms in cities scattered all across the US databases for sale on the Dark Web.
- Hackers are offering access to a law firm's entire network for as low as \$3,500.
- A criminal could use the info to trade on insider information, insurance fraud, among other things, says research firm.
- Sophisticated hackers are selling access on the Surface Web as well as the Dark Net.

Source: <https://www.cnbc.com/2018/07/11/hackers-selling-access-to-law-firm-networks-on-dark-web-sites.html>

CONFIDENTIAL AND PROPRIETARY

FA



You Are a Target!

THE FLORIDA BAR

[ABOUT THE BAR](#)[NEWS & EVENTS](#)[FOR THE PUBLIC](#)[MEMBER SERVICES](#)[LOG IN](#)[FIND A LAWYER](#)

[THE FLORIDA BAR](#) / [About the Bar](#)

Search:

Go

The Florida Bar News

[Advertising Rates](#) • [Classifieds](#) • [Attorneys Exchange](#) • [Archives](#) • [Subscribe](#) • [Journal](#)

June 2, 2016

  [News HOME](#)

New email scam alert!

[Share](#) [Tweet](#) [LinkedIn](#)

The Florida Bar warns its members about more fraudulent emails that are being distributed; one with the subject "Florida Bar Complaint - Attorney Consumer Assistance Program," another "Florida Bar Notification," and the latest "Lawyers and judges may now communicate through the portal."

Do not click on any links contained within the emails and delete them immediately. It is suspected that these emails contain links to malicious software.

The "Florida Bar Complaint" fraudulent email bears the name of Bar President-elect William J. Schifino, Jr., on behalf of the Attorney Consumer Assistance Program (ACAP), and it informs members that a complaint has been filed against their law practice. If you have any questions about Bar complaints, call ACAP at 866-352-0707. If a Bar complaint has been filed against a member, the Bar will not initiate contact with that member via email.

Another email bears the name of a Board of Governors' member and says The Florida Bar "fees and payment schedule has changed." There is also a reference to adding a new "Virtual Business Card System" and asks members to review the information and provide the most current information available. This email should be deleted and the links to the attached PDF files should not

CONFIDENTIAL AND PROPRIETARY





Case Study: Dentons Money Wiring Scam



- \$2.52 Million Fraudulent Wire Transfer
- 2017 Real estate transaction with Timbercreek Mortgage
- Dentons received emails from people who appeared to be affiliated with Timbercreek.
- Emails indicated that one of Timbercreek's accounts was subject to an audit and asked for Dentons to send the money to an international account in Hong Kong, held by a third-party called Yiguangnian Trade Co. Ltd.
- The Dentons side attempted to verify, leaving a voicemail at Timbercreek and seeking letters of authorization from the mortgage servicer and the Yiguangnian entity
- Received what appeared to be authorized letters from both parties.
- Although Dentons didn't receive a phone call back, it did receive what appeared to be authorization letters from Timbercreek and Yiguangnian decided to go ahead with transfer
- Several weeks passed, and Timbercreek wanted to know what happened to its money. That's when an associate realized that millions of dollars had been sent to a scam account.
- Denton's was able to recover a few hundred thousand dollars. Insurance coverage was denied because this situation doesn't fall under the computer fraud rider to the firm's policy.

<https://abovethelaw.com/2019/01/biglaw-firm-duped-into-wiring-money-to-scam-account-loses-2-5-million-in-cyber-breach/>





Ethical Concerns

- You are a custodian of sensitive data
 - Financial Records
 - Medical Records (HIPAA)
 - Private and (potentially) damaging information
 - Credit Card Information (PCI)
- 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 your data security?
- Do you have an Incident Response and/or Data Breach plan?
- Do you have a Disaster Recovery – Business Continuity Plan in place?





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.





Pillar 3 - Privacy & Information Security

- Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.
 - Physical security of Non-public Personal Information
 - Network security of Non-public Personal Information
 - Disposal and Maintenance of Non-public Personal Information
 - Establish a disaster management plan
 - Appropriate management and training of employees to help ensure compliance with Company's 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



Pillar 3 - Privacy & Information Security

- Practical Suggestions

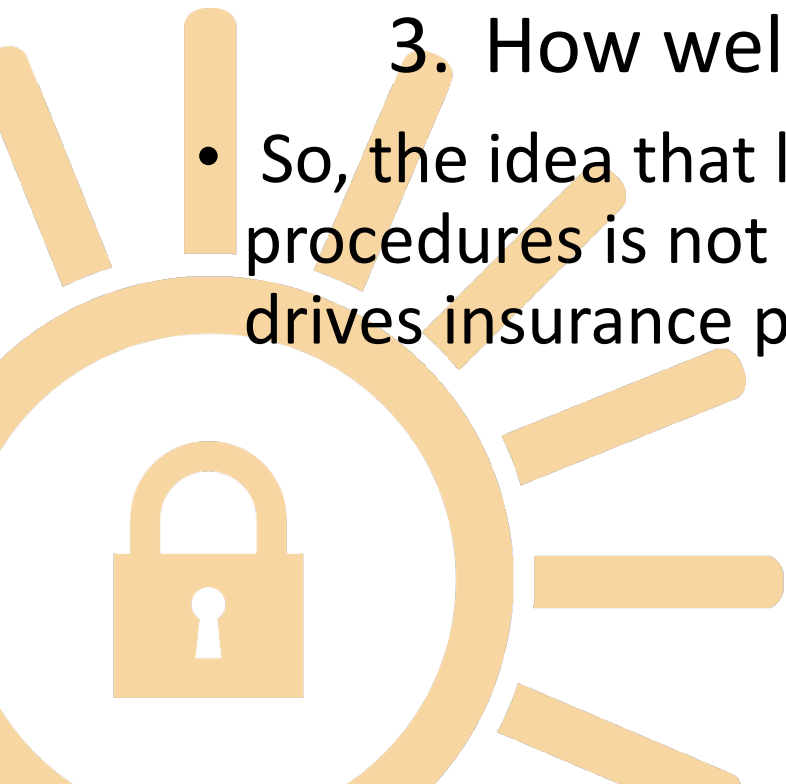
- Establish a process to use strong passwords that change frequently
- Close paper and electronic files containing NPI when away from the desk
- Secure points of entry to buildings and offices
- Appropriate firewalls within computer network system
- Policy for independent service providers stating protection of NPI is their responsibility when documents are in their possession





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.





Florida Information Protection Act - FIPA (State)

- Florida Information Protection Act, Sec. 501.171, F.S.
 - Defines a security breach
 - Covered entity must give notice to each individual in Florida whose private information was, or which the entity reasonably believes to have been, accessed as a result of a security breach
 - Covered entity must provide notice to the Department of Legal Affairs of any security breach affecting 500 or more Florida individuals
 - Notification to Consumer Reporting Agencies required if security breach affects more than 1,000 persons at a single time

What is PII

- First & Last Name and one of:
 - SSN
 - Financial Account Number
 - Government ID number
 - Health Information or Insurance ID
- Username or Email Address, including password or security questions
 - Encrypted passwords are not considered PII!



Problem

1

Hackers are now targeting Law Firms due to the sensitivity of data and lack of security measures deployed by a majority of law firms.

2

Federal and State Compliance Regulators are beginning to enforce cybersecurity mandates on Law Firms and imposing civil penalties due to increased number of cyber breaches.

3

Cybersecurity Awareness and Education is severely lacking in the Law Firm space, perceived to be hard to implement and expensive. **Another common misperception is their IT managed service provider has them covered.**

How are Law Firm's dealing with the Cyber Theft Epidemic today...



CONFIDENTIAL AND PROPRIETARY

FA



Not Much



Ignore the problem and hope it goes away





Panic



Spend all the right money in all the wrong places



Where do you fall?



Nothing

Ignore the problem and hope it goes away



Panic

Spend all the right money in all the wrong places



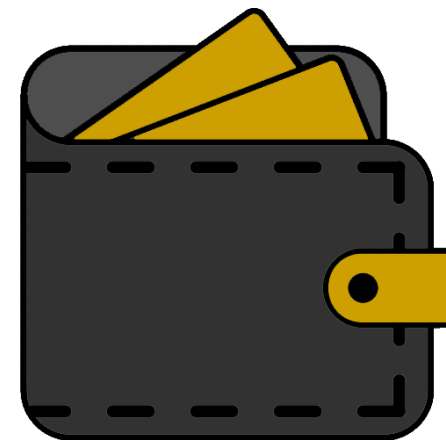
Primary Objectives



Avoid Compromise
Costs and Brand Damage



Achieve Compliance
Follow the Law and Avoid Fines



Affordable Solutions
Custom Designed for SMBs



The Right Approach



Evaluate, Identify, and Manage Risk





SRA Methodology

How we help our clients evaluate, identify, and manage risk...



NIST SP800-30 provides the Risk Assessment Methodology for all federal agencies to follow.

The private sector uses NIST as the foundation for all security controls and compliance frameworks in the US.

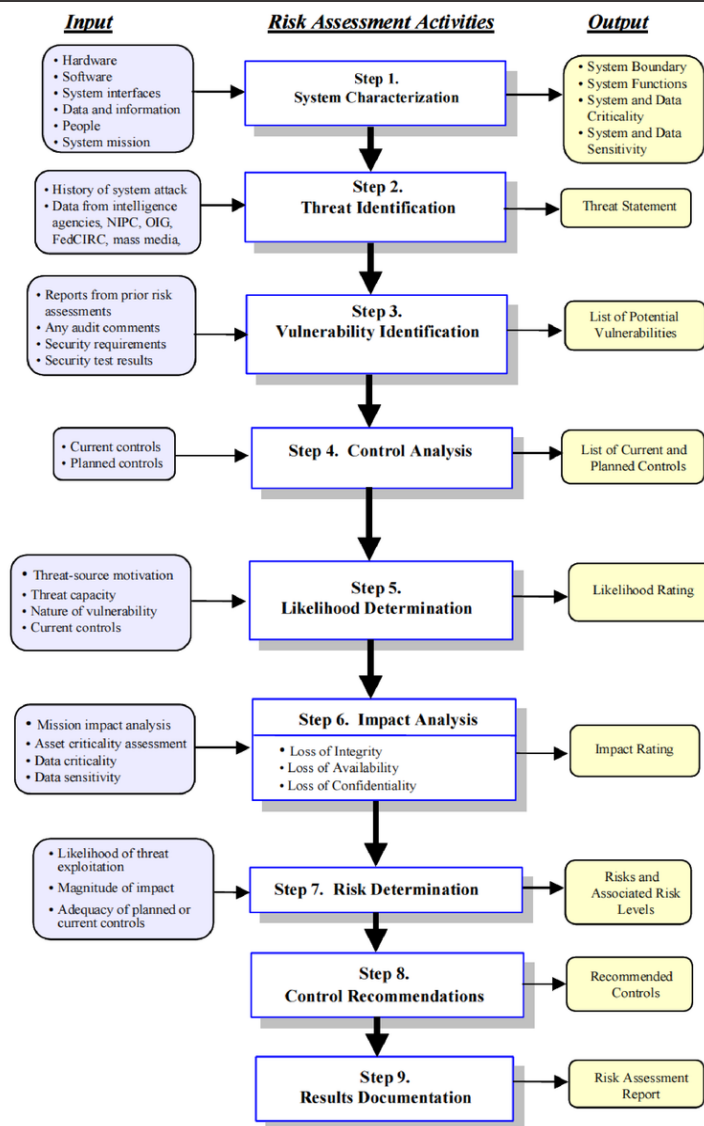


Figure 3-1. Risk Assessment Methodology Flowchart





NIST Based Compliance Frameworks

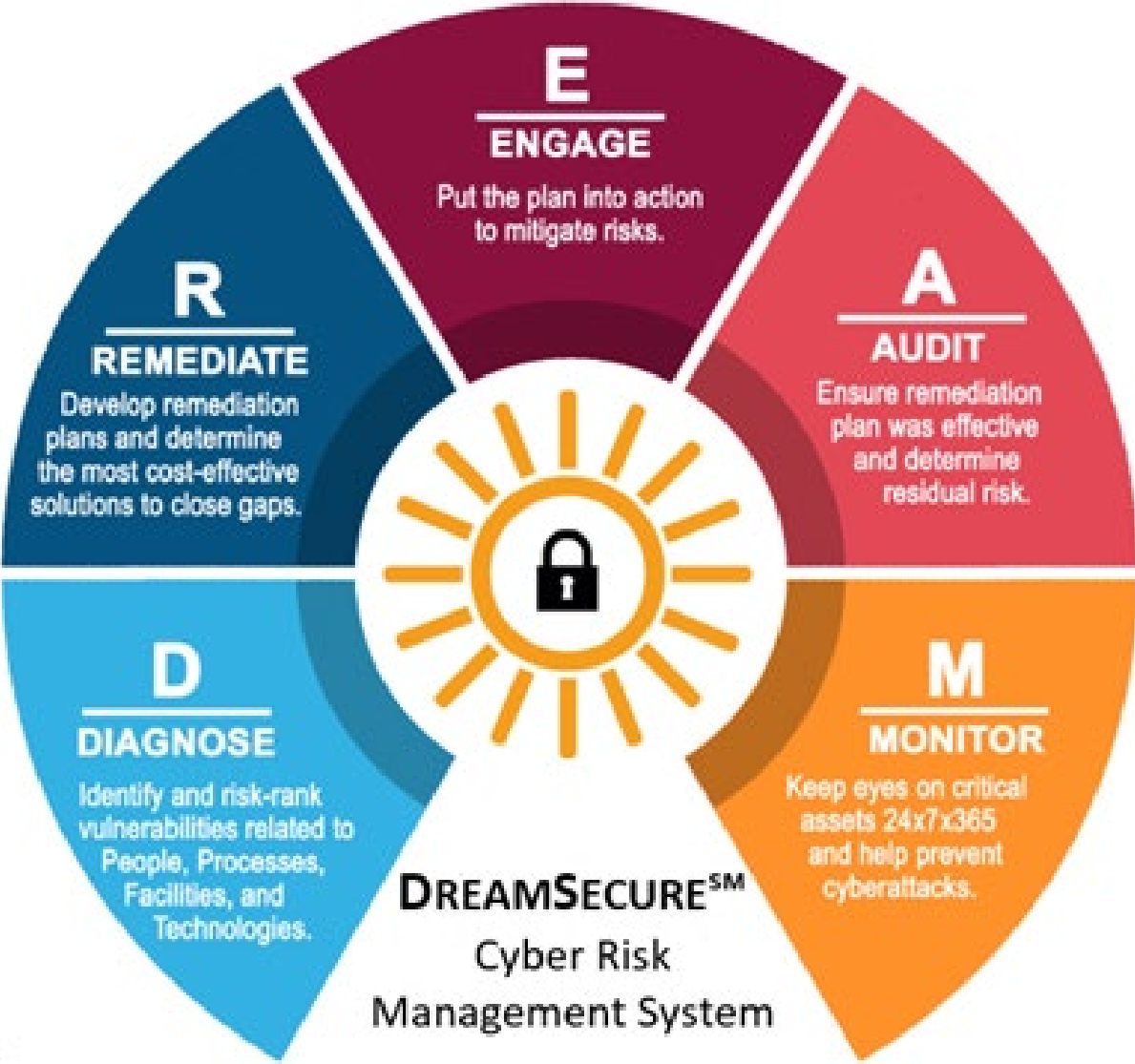
NIST SP800-53 rev.5 - provides a catalog of security controls for all U.S. federal [information systems](#) except those related to national security.





Adopt a Cyber Risk Management System

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





Types of Assessments

- **Security Risk Assessment**

- Analyze the risk profile of your organization; develop actionable and prioritized remediation strategies.

- **Compliance Assessments**

- Identifies gaps specific to a compliance framework that a company must adhere to
- PCI-DSS, HIPAA/HITECH, HITRUST, ISO 27001, SOC, GLBA, FISMA, FedRAMP, GDPR

- **Vulnerability Assessment (scheduled)**

- Automated and manual scanning on internal and external assets to find known vulnerabilities.

- **Penetration Testing**

- Ethical hacking to attempt to gain access to your organization's networks and data.

- **Threat Modeling and Architecture Reviews**

- Comprehensive attack simulation based on current or planned network architectures.



Security Risk Assessment

- Classify all sensitive information (electronic and paper)
- Perform Comprehensive Inventories
 - Inventory all hardware & software in use or in storage
 - Inventory ALL cloud services (there are more than you think)
 - Inventory ALL partners you do business with
- “Footprint” your organization’s IT infrastructure
- Assess from the outside-in, and inside-out for best practices
 - Think like a hacker!
- Perform a Qualitative or Quantitative Risk Analysis
 - e.g. Impact / Likelihood
- Decide on security controls to cover your highest areas of risk
- Schedule the implementation of all controls
- Repeat as changes are made; formal assessment at least annually!

Sample SRA Report

Security Risk Assessment

Final Report

Johnson Cardiology

8 May 2016



TABLE OF CONTENTS

Executive Summary	1
The Approach	2
Kickoff	2
Assessment	2
Report	3
Project Management	4
Scope of Engagement	4
Stakeholder Registry	4
Schedule of Events	4
Security Risk Assessment	5
Security Compliance Assessment	6
Administrative Safeguards	6
Physical Safeguards (Truncated)	9
Technical Safeguards (Truncated)	9
Organizational Requirements (Truncated)	9
Policy and Procedure Requirements (Truncated)	9
Plan of Actions and Milestones (POA&M)	10
Appendix A: Implementation Guidance	11
Encryption (Bitlocker)	11
Encrypting Thumbdrives	13
Creating New Users	14
Removing Administrative Privileges	14
Enforcing Complex Passwords	14
Installing Advanced Malware Protection (GSS)	14
Installing Remote Tracking Software	14
Appendix B: Vulnerability Scan Results	15

www.GoldSkySecurity.com



FA



Sample – Risk Analysis

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
Malware infiltration on networked devices Malware-directed internal reconnaissance	External Adversarial Internal Adversarial Internal Non-Adversarial	(1) Inconsistent use of AntiMalware software (2) Malware events not continually monitored (3) Local administrative users can disable malware detection (4) AntiMalware not deployed on server platforms	(1) Anti-Malware deployed on most workstations	Very High	Moderate	High	High	High
Exploit vulnerabilities on internal organizational information systems	External Adversarial Internal Adversarial	(1) No vulnerability management processes in place (2) No endpoint best practice policies applied to workstations or servers	Automatic updates help to prevent many vulnerabilities	High	Moderate	Moderate	Very High	High
Conduct Denial of Service (DoS) attack.	External Adversarial	No D/DoS services or firewalls in place	None	High	High	High	High	High



Sample – Compliance Analysis

Citation	(R/A)	Title	Description	Assessment	Recommendation	Status	Risk
164.308(a)(1)(ii)(A)	R	Risk analysis	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 or business associate.	No security risk assessments have been performed.	Perform a formal security risk assessment annually, or whenever major network/compute changes occur.	Finding	High
164.308(a)(1)(ii)(B)	R	Risk Management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Risks are presently unknown and therefore not controlled	(1) Perform a formal security risk assessment annually, or whenever major network/compute changes occur. (2) Perform continual risk management using the SRA as guidance	Finding	High
164.308(a)(1)(ii)(C)	R	Sanction Policy	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Sanctions are listed in security Policy	Add a sanctions policy in your acceptable use policy	Not a Finding	Low
			Implement procedures to regularly	Truncated	Truncated		



Sample – Remediation Roadmap

Citation / Risk Area	Recommended Remediation	Assigned To	Due By	Completed On
164.308(a)(1)(ii)(A)	Perform annual risk analysis	A. Carter	5/7/2016	5/7/2016
Malware Defense	Implement advanced malware defense on all computers	A. Carter	30 Days	5/7/2016
Data Loss & 164.312(e)(2)(ii)	Update all computers to Windows 8 Pro or Windows 10 Pro and enable Bitlocker	A. Carter	60 Days	
Passwords & 164.308(a)(5)(ii)(D)	Enable passwords with standard windows complexity for all users	A. Carter	30 Days	
User Management	Create a unique user account for all users	J. Harrison	60 Days	
Least Privilege & 164.312(a)(2)(i)	Remove administrative user permissions from all computer non-admin staff.	J. Harrison	90 Days	
-- Truncated --				

Cybersecurity Tips



CONFIDENTIAL AND PROPRIETARY





Cybersecurity Tips

1. Define what your critical data is and where it should be stored
2. Have written security policies and procedures in place to protect critical data
3. Purge data you don't need
4. Secure the data on encrypted drives or media
5. Secure your hardware with complex (unique) passwords
6. Set an automatic screensaver lock
7. Always run Anti-Malware software
8. Always install the latest OS and software updates
9. Stay updated through cybersecurity awareness training
10. Deploy VPN & MFA wherever possible
11. Have a plan!



And remember...

PASSWORDS ARE LIKE UNDERPANTS



Change them often, keep them private and never share them with anyone.

Thank you for your time and attention today!