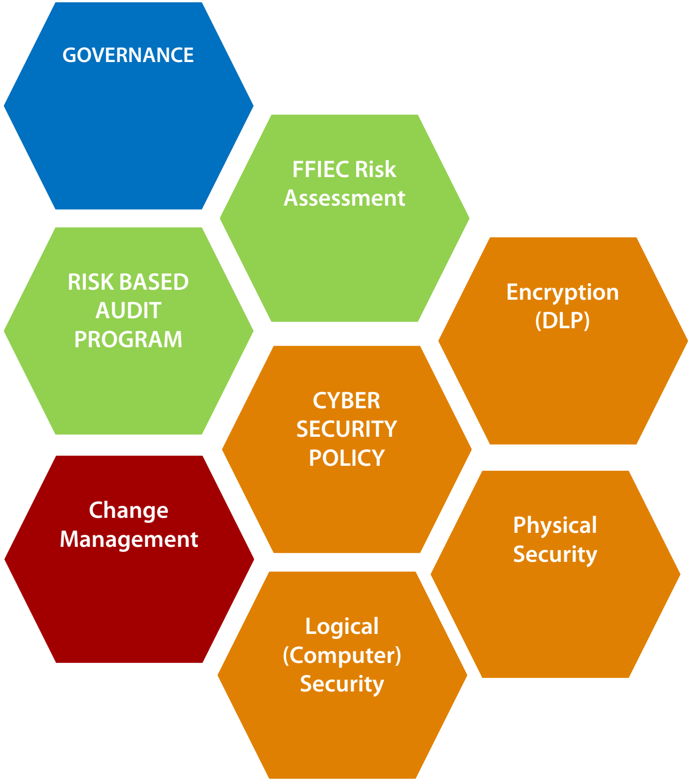


GOVERNANCE

FFIEC Risk Assessment

RISK BASED AUDIT PROGRAM

Encryption (DLP)

CYBER SECURITY POLICY

Change Management

Physical Security

Logical (Computer) Security

Building a **Solid** Cyber**security** **Foundation**

NACUSO Las Vegas
April 4, 2016

PLATINUM PARTNER

CU*ANSWERS
A Credit Union Service Organization

Your **Presenter**

Patrick Sickels, CU*Answers

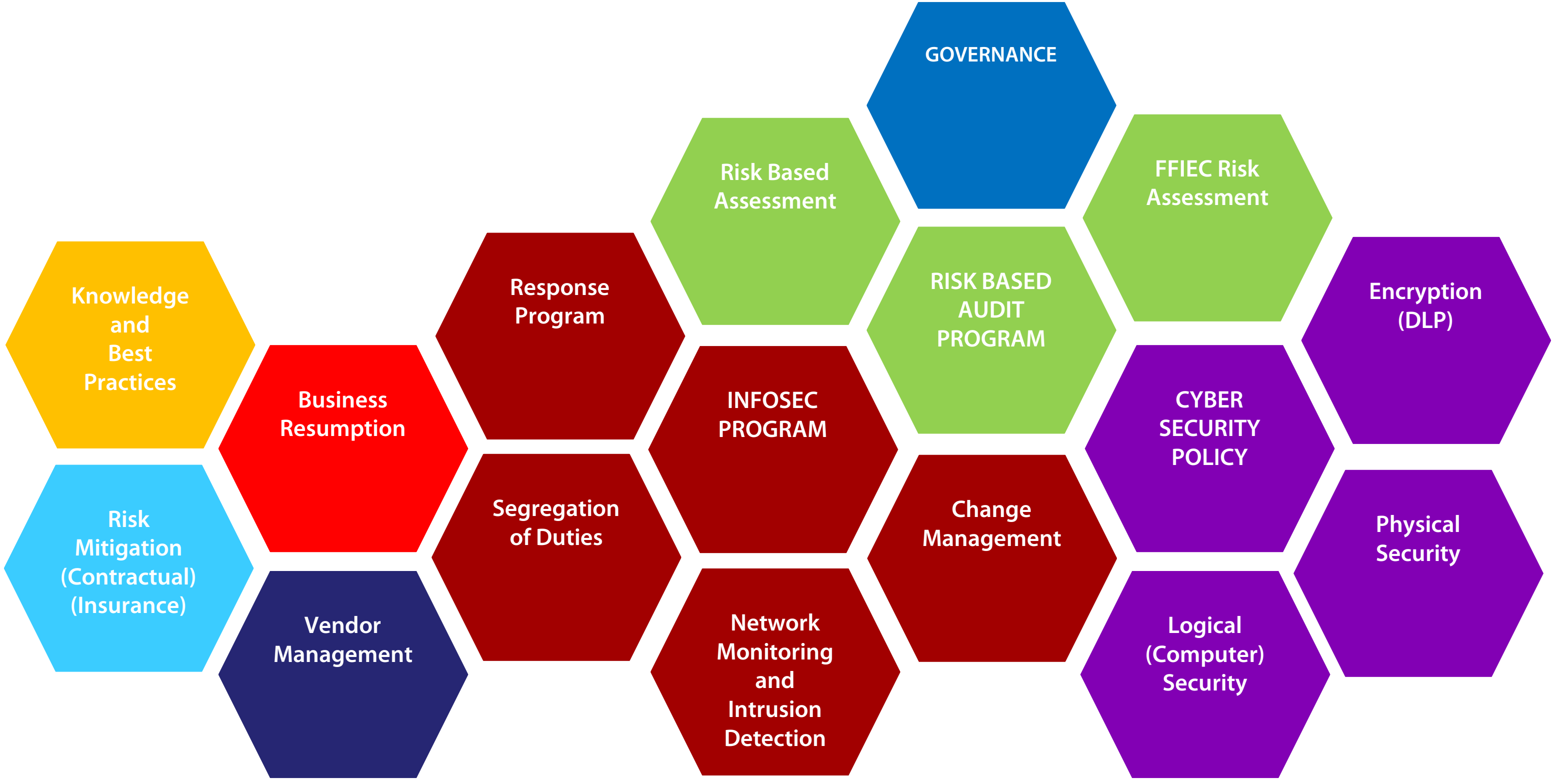
Internal Auditor for 9 years

Financial Compliance for 6 years

Attorney in Michigan

Member of ISACA

Cybersecurity **Fundamentals**



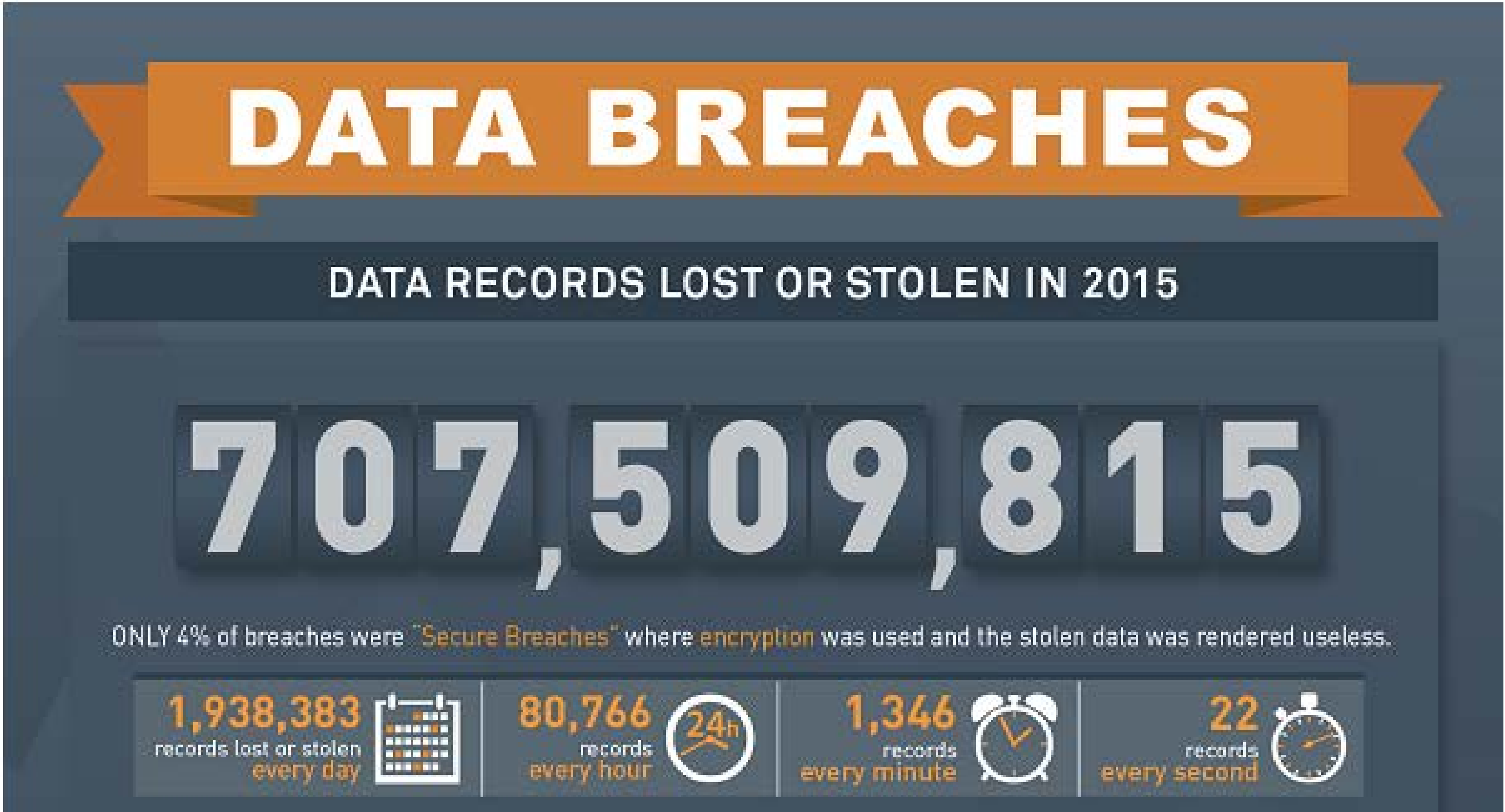
Old Wine **New Bottles**

Fundamental Position of CU*Answers is that **Cybersecurity** does not fundamentally alter the requirements of protecting member information.

When do you need a **Cybersecurity Program?**

Personally Identifiable Financial Information of Members

Trade Secrets or other Privileged Information from a Financial Institution



DATA BREACHES

DATA RECORDS LOST OR STOLEN IN 2015

707,509,815

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

1,938,383 records lost or stolen every day	**80,766** records every hour	**1,346** records every minute	**22** records every second

Source: gemalto

Credit Unions: **Industry Stats**

2015 largest credit union breach:

Winston-Salem based Piedmont Advantage CU ($308M)

Had to notify 46,000 members of a missing laptop that contained PII

2014 Average spend on Cybersecurity: $136K (source: NAFCU)

2014 Average spend costs associated with merchant data breaches: $226K (source: NAFCU)

Source: CU Times/ Safenet

Notification law is based on where the **member resides**

CFPB: **UDAAP (Unfair/Deceptive Practice)**

2016 first action by CFPB on cybersecurity:

Online payment processor
Accused of lying about PCI Compliance
Accused of lying about their security procedures (encryption)
Released apps without testing security

Fined $100,000
Cease and Desist Order
Fix application release process

FTC claims the same authority (Wyndam Hotels)

Source: CFPB

Oversight and **Reports**

Governance

“Does the board of directors approve of and oversee the development, implementation, and maintenance of the program, including assigning specific responsibility for its implementation and reviewing reports from management?”

On an **annual** basis, make sure the **Board Minutes** reflect that the Information Security (and Cybersecurity Policy) were **approved** by the board. What else?

Oversight and **Reports**

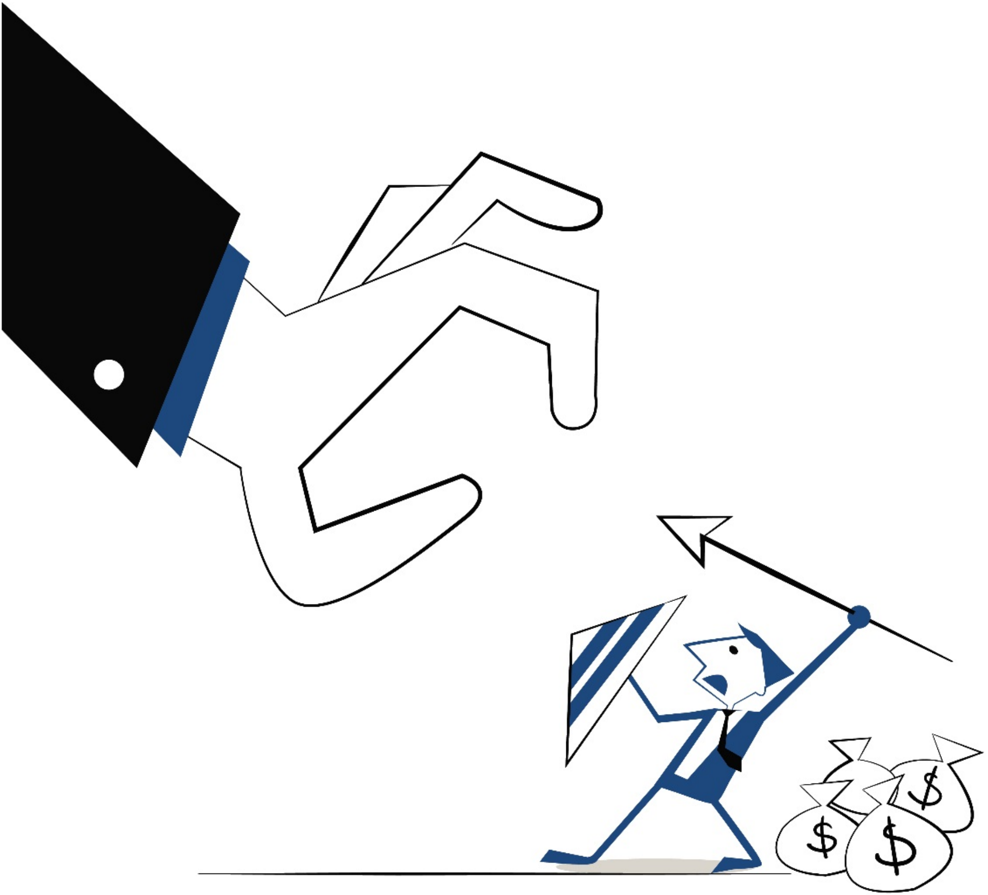
Reports of Policy Violations

Reports of Incident Responses

Reports of Internal and External Audit Exceptions

Oversight and **Reports**

Governance



Remember, it is okay to fight (especially when it comes to business)

Oversight and **Reports**

Cyber Security Policy

InfoSec Program

Comprehensive **InfoSec Plan**

“. . . a comprehensive **written** information security program including **administrative**, **technical**, and **physical** safeguards appropriate to the nature and scope of its activities“

Add the word **Cybersecurity** to your InfoSec Plan or even create a brand new Cybersecurity Policy. Your Cybersecurity Policy can state what your **employees** are responsible for.

Cyber Security Policy

InfoSec Program

Comprehensive **InfoSec Plan**

"… ensure the security and confidentiality of member information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in **substantial harm or inconvenience to any member**"

Logical (Computer) Security

Logical **Access Controls**

“… Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means”

Identify systems with member info

Regularly determine who has access

Reasonably remove access in a timely fashion

Physical **Access Controls**

"… Access restrictions at physical locations containing member information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals"

- Identify physical locations with member data
- Regularly determine who has access
- Reasonably remove access in a timely fashion

Encryption
(DLP)

Data **Encryption**
Data **Loss Prevention**

"… Encryption of electronic member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access"

Encryption Controls for Sending (email)

Encryption Controls for at Rest

USB Ports
CD-W
Email
Detection

Intrusion **Detection and Prevention**

"… monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems"

Intrusion detection systems work by either looking for signatures of known attacks or deviations of normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer.

Change Management

System **Modifications**
Change **Controls**

“. . . Procedures designed to ensure that member information system modifications are consistent with the … information security program”

Do you patch? (One of the **most important**)

System checklists (Server builds)

Change management doesn’t **override** security

Segregation of **Duties**

"… Dual controls procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information"

Background Checks

Segregation of Duties

Dual Controls

Segregation of Duties

Terry **Childs**

Network Manager for the City of San Francisco

Designed their FiberWAN and even received a copyright for it

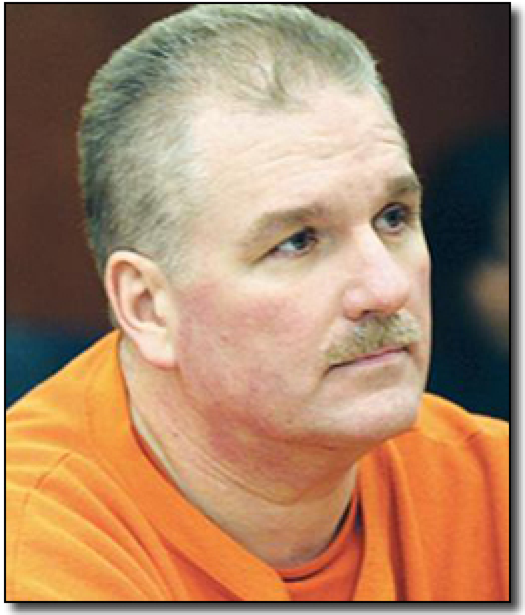
Was the **only** person with passwords, and the only person who could support it (completely protective of his turf)

Network was being audited without his knowledge (he claimed theft and intrusion by the security professional doing the audit)

They demanded the usernames and passwords for the network and **he would not give the passwords to the city**

He was arrested and finally gave the information directly to the Mayor, who visited him in his cell

Sentenced to four years on a felony account of computer tampering, and ordered to pay $1.5m in fines



Response **Program**

“. . . Response programs that specify actions to be taken when … unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies”

Notify Clients

Notify Vendors

Notify Law Enforcement

Business **Resumption**

“. . . Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures”

Environment Protection (fire, moisture, heat)

Backups (restoration in time and restoration far enough back)

Testing the Plan at least annually

Six Lines of **Code**

Business Resumption

Tim Lloyd was an 11 year network engineer with Omega Engineering

He was angry at a demotion and was eventually fired for insubordination

He wrote six lines of code that deleted all of Omega's software

Omega did not have sufficient backups

Omega stayed in business but laid off 80 employees and lost $10 million in sales

```
1. 7/30/96
2. F:
3. F:\LOGIN\LOGIN 12345
4. CD \PUBLIC
5. FIX.EXE /Y F:\*.*
6. PURGE F:\ /ALL
```

Vendor **Management**

"… Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures"

Environment Protection (fire, moisture, heat)

A Business Resumption **Plan**

Testing the Plan at least annually

Cyber Liability **Insurance**

Risk
Mitigation
(Contractual)
(Insurance)

We will not give an opinion on the quality of a particular carrier's insurance. Our recommendation is to ensure that your organization has a clear understanding of:

- **Coverage (example: member notification)**
- **Exclusions (very critical)**
- **Payout triggers**
- **Carrier control**
- **Limitations**
- **Deductibles**

Knowledge and **Best Practices**

Cybersecurity Resources

http://www.cuanswers.com/resources/cybersecurity/

Knowledge and **Best Practices**

Cybersecurity Resources

Knowledge and **Best Practices**

Cybersecurity Resources

CU*Answers Cybersecurity Policy (PDF)

CU*Answers Information Security Policy (PDF)

CU*Answers Acceptable Use Policy (PDF)

Cybersecurity Policy Template for Credit Unions (Word)

Information Security Program for Credit Unions (Word)

Acceptable Use Policy Template for Credit Unions (Word)

Knowledge and **Best Practices**

Cybersecurity Resources

The Critical Security Controls for Effective Cyber Defense Version 5.0

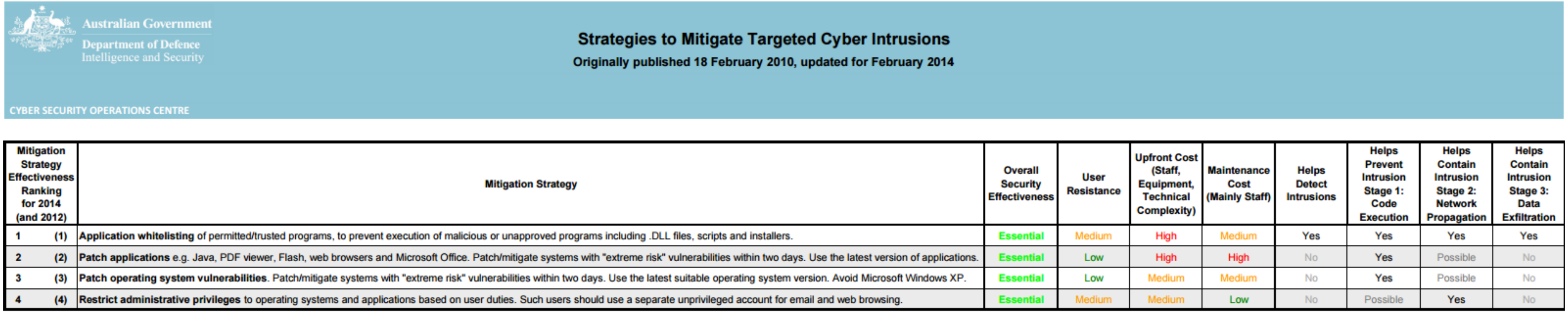
COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

https://www.sans.org/media/critical-security-controls/CSC-5.pdf

Knowledge and **Best Practices**

Cybersecurity Resources

Knowledge and Best Practices



Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

Strategies to Mitigate Targeted Cyber Intrusions

Originally published 18 February 2010, updated for February 2014

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1 (1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2 (2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3 (3)	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4 (4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

Cybersecurity **Checklist**

Knowledge and Best Practices

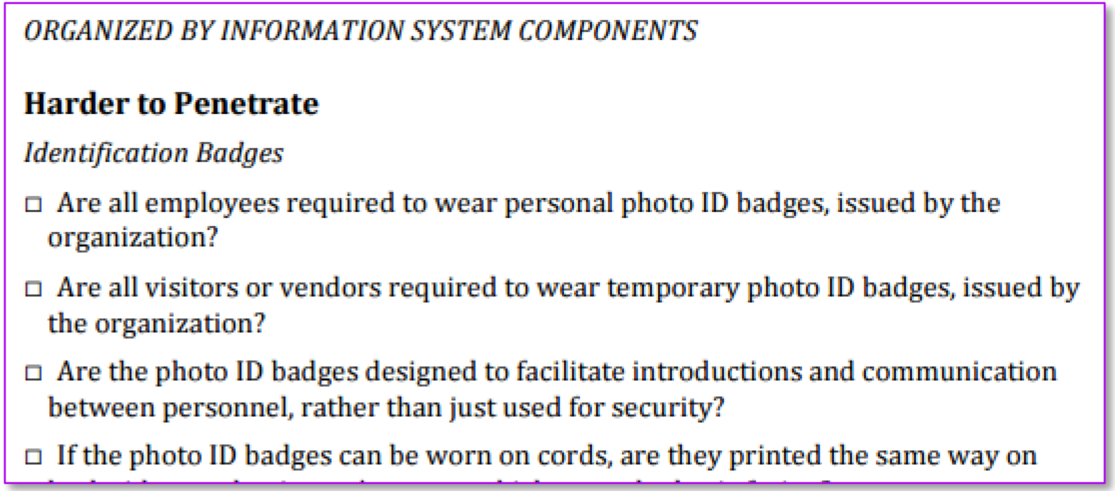
Plain-language checklist

Basic controls to protect systems and data
Easy to understand

Not an official standard, but one we need to pay attention to

Over 1,000 items

Usccu.us



ORGANIZED BY INFORMATION SYSTEM COMPONENTS

Harder to Penetrate

Identification Badges

□ Are all employees required to wear personal photo ID badges, issued by the organization?

□ Are all visitors or vendors required to wear temporary photo ID badges, issued by the organization?

□ Are the photo ID badges designed to facilitate introductions and communication between personnel, rather than just used for security?

□ If the photo ID badges can be worn on cords, are they printed the same way on

Incident Response: **Tactics**

Knowledge and Best Practices

Test the plan before a breach

Identify the breach response team

Have a communications plan locked and loaded

Understand regulations and contracts
that govern post-breach obligations

Determine what experts you will engage in advance

Respond in an “all out fashion” when breach detected

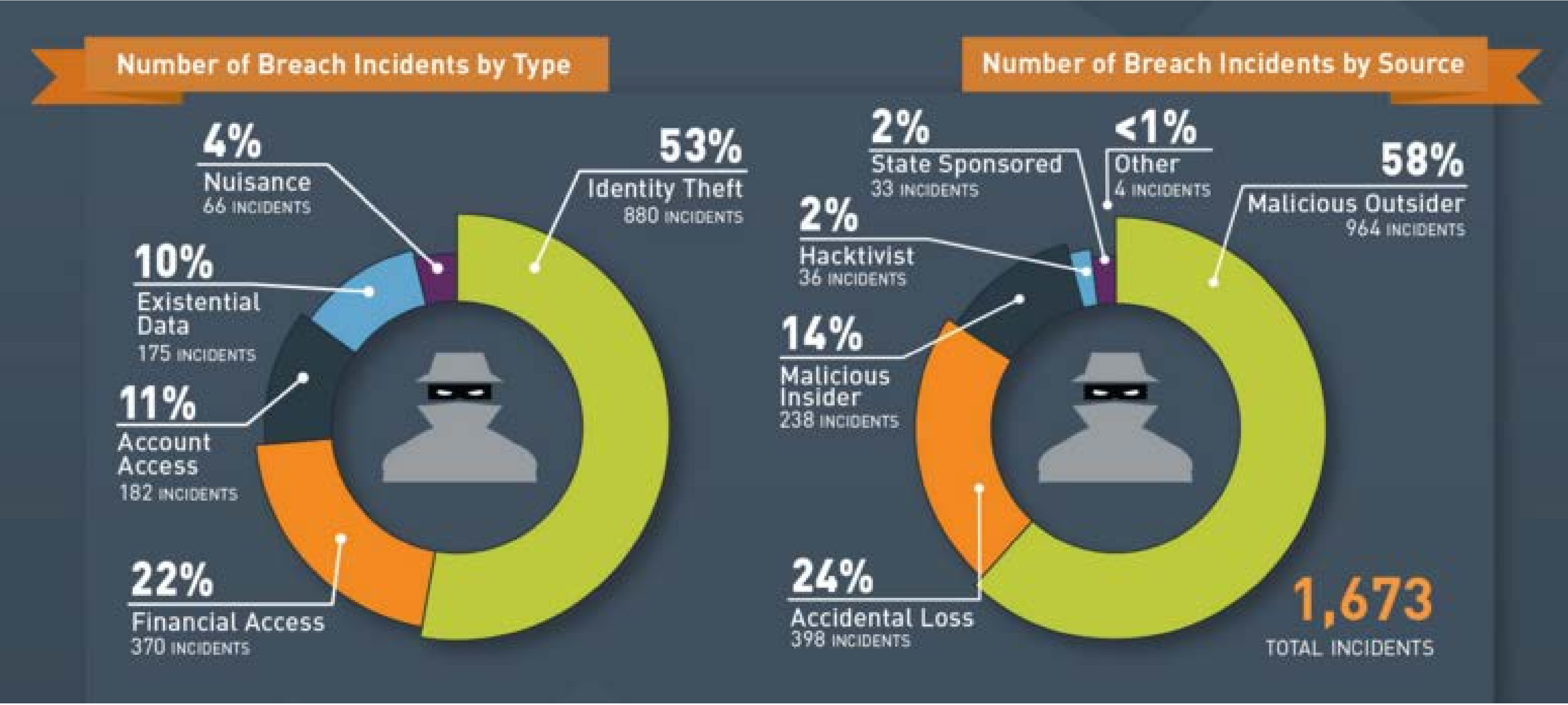
Preserve evidence
Engage insurance carrier
Engage regulators and law enforcement early

Data Breach Response Guide

By Experian® Data Breach Resolution
2013-2014 Edition

Trust the Power of Experience.

Experian®

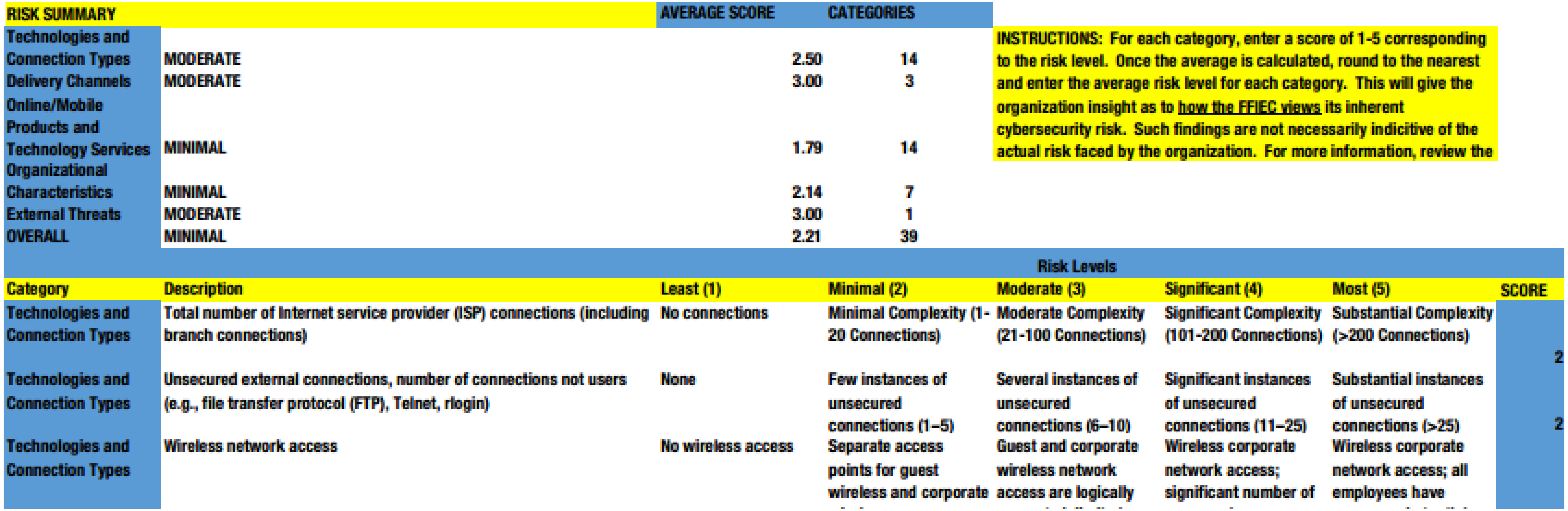


Source: gemalto

FFIEC **Cybersecurity Tool**

FFIEC Risk Assessment

Risk Matrix



RISK SUMMARY		AVERAGE SCORE	CATEGORIES
Technologies and Connection Types	MODERATE	2.50	14
Delivery Channels	MODERATE	3.00	3
Online/Mobile Products and Technology Services	MINIMAL	1.79	14
Organizational Characteristics	MINIMAL	2.14	7
External Threats	MODERATE	3.00	1
OVERALL	MINIMAL	2.21	39

INSTRUCTIONS: For each category, enter a score of 1-5 corresponding to the risk level. Once the average is calculated, round to the nearest and enter the average risk level for each category. This will give the organization insight as to how the FFIEC views its inherent cybersecurity risk. Such findings are not necessarily indicitive of the actual risk faced by the organization. For more information, review the

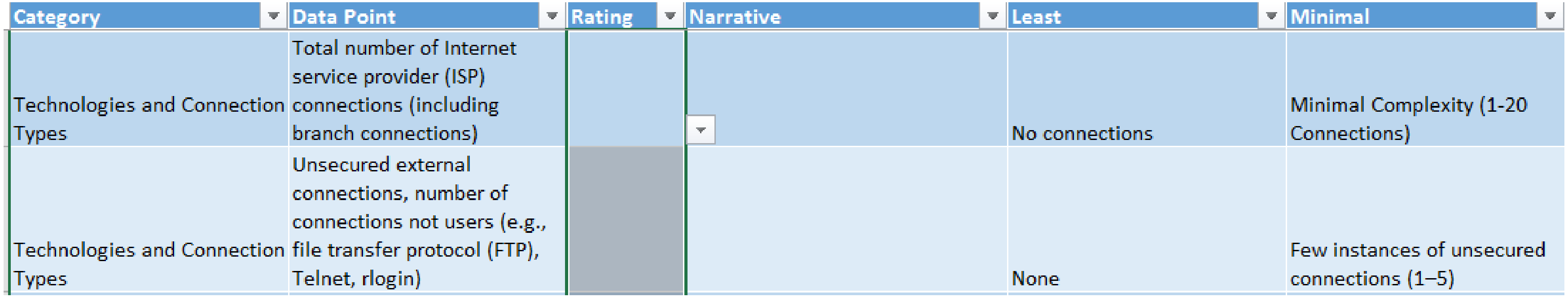
		Risk Levels					
Category	Description	Least (1)	Minimal (2)	Moderate (3)	Significant (4)	Most (5)	SCORE
Technologies and Connection Types	Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal Complexity (1-20 Connections)	Moderate Complexity (21-100 Connections)	Significant Complexity (101-200 Connections)	Substantial Complexity (>200 Connections)	2
Technologies and Connection Types	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)	2
Technologies and Connection Types	Wireless network access	No wireless access	Separate access points for guest wireless and corporate	Guest and corporate wireless network access are logically	Wireless corporate network access; significant number of	Wireless corporate network access; all employees have	

http://www.cuanswers.com/wp-content/uploads/FFIEC-Cybersecurity-Assessment-Inherent-Risk-Base-Worksheet.xlsx

FFIEC **Cybersecurity Tool**

FFIEC Risk Assessment

Maturity Models



Category	Data Point	Rating	Narrative	Least	Minimal
Technologies and Connection Types	Total number of Internet service provider (ISP) connections (including branch connections)			No connections	Minimal Complexity (1-20 Connections)
Technologies and Connection Types	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)			None	Few instances of unsecured connections (1–5)

http://www.cuanswers.com/wp-content/uploads/FFIEC-Cybersecurity-Assessment-Tool-2.xlsx

FFIEC **Cybersecurity Tool**

Maturity Models

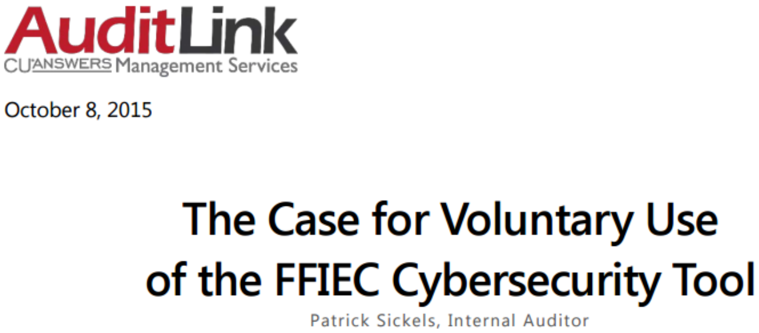
First of all, the Maturity Model statements are not well correlated to the risks identified in the FFIEC Inherent Risk Tool.

Second, there is a significant amount of arbitrariness in the ranking of the various Maturity levels. (The FFIEC requires that a financial institution meet all of the categories of one Maturity before moving on to the next level). For example, to get to the "Advanced" Maturity of Oversight, an institution must be able to answer affirmatively that "The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy." This requirement is not well thought out and does not seem to have a clear relationship to cybersecurity. Clarity of expected output is missing in many of the Maturity Tool statements.

In addition, there are certain categories that do not appear at all to be relevant in the credit union space. Very few credit unions will be able to answer that "Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components."

FFIEC **Cybersecurity Tool**

Maturity Models



AuditLink
CU ANSWERS Management Services

October 8, 2015

The Case for Voluntary Use of the FFIEC Cybersecurity Tool

Patrick Sickels, Internal Auditor

http://www.cuanswers.com/wp-content/uploads/The-Case-for-Voluntary-Use-of-the-FFIEC-Cybersecurity-Tool-v2.pdf

Breach Prevention or **Breach Management?**

The evidence shows breaches cannot be stopped

Prevention strategies are still important but in 2016 the focus and priorities will shift to breach acceptance strategies

Breach Acceptance Tactics/Perspective:

1. Incident Response Plan Priority
2. Data security centric
3. Sliding scale authentication strategies
4. Refocus on the endpoint

Incident Response: **Data Security Centric Tactics**

Data will be moved across systems

- Containing data reduces value to end users
- Think "Big Data" / "Data Warehouses" / Cloud computing

Encryption of PII data

- PII data that has been encrypted is less valuable to attackers
- Increasing the cost of attacking your organization will significantly reduce the threat of a breach (attackers have costs, too).
- Encrypt PII data everywhere it is at rest (i.e. stored), regardless of system
- Encrypt PII data motion on the network

Encryption: **“Gotchas”**

Encryption increases the cost of an attack – that’s good

Encryption increases costs to the organization – that’s reality

- Key management – protecting the material that encrypts the data
  - Do you have a key management policy?
  - How do you keep key material secure / private?
- Encryption is under attack
  - SSLv2; SSLv3, TLS, SSH, etc.
  - Successfully attacking even weak encryption is still hard
- Encryption requires maintenance
  - Patching / Compatibility issues
  - Moving to new forms is expensive and requires coordination with members/partners
- Network security devices (firewalls/IDS/IPS) can’t inspect encrypted traffic for threats

Data Breach Management:
User Authentication/Access Tactics

More authentication types than we can shake a stick at (passwords, biometrics, one-time passwords, cell phones, USB sticks, etc.)

A data-centric perspective on security:

- Authentication barriers based on the context of the user action
- Layers of authentication based on the risk
- Sliding scale of authentication barriers based on the risk of the request/transaction

Outsourcing authentication

- Can outside experts make authentication decisions more accurately than we can?
- Will members demand external authentication (cell phones, google authenticator, etc.?)
- How will internal/external authentication processes be layered/implemented?

User Authentication Tactics: **Your Network**

When will we shift to sliding-scale risk based authentication for internal/network users?

When will passwords be relegated to low-risk activities only?

Readily available systems can compromise 19 character passwords in less than 3 weeks (low cost to attacker)

27% of US employees would sell their passwords for $1,000 or less (source: Sailpoint.com survey)

Password strength is NOT improving (#1 password is still 123456 and #2 is password)

What you will budget over the next 3 years to implement a tactic to address this concern

Breach Management: **Refocus on the Endpoint**

Users interact with PII at the workstation/PC/laptop (endpoint)

Bad actors are targeting the workstation to exfiltrate PII

They will also target mobile devices in hopes they'll find your PII there

They are overwhelming traditional AV solutions with sheer volumes of malware

You need a plan for assessing workstation security and addressing weaknesses in 2016

Breach management: **Mobile Strategies**

Have a policy that governs use of mobile devices and PII

Implement technical controls that can wipe mobile devices

Audit mobile devices against the policy and software updates

Educate users on security best practices

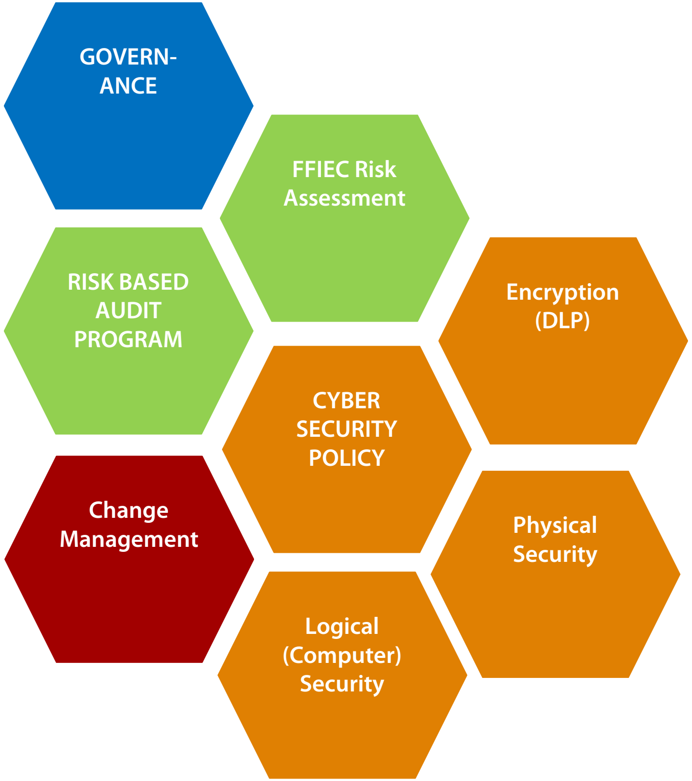
Pros and Cons of **Cloud Computing**

Pros

- Low start up costs
- Automatic software upgrades
- Ease of use
- Ease of access – internet connection
- Scalability – provided by cloud provider
- Security – cloud providers like Microsoft take it seriously

Cons

- Subscription based pricing means you're never done paying
- Less flexibility
- Security – lack of visibility into what's happening under the covers
- On site technology not eliminated – still require some infrastructure



GOVERN-ANCE

FFIEC Risk Assessment

RISK BASED AUDIT PROGRAM

Encryption (DLP)

CYBER SECURITY POLICY

Change Management

Physical Security

Logical (Computer) Security

Questions?