

BUILDING **EFFECTIVE** INTERNAL CYBER POLICIES AND PROCEDURES

PATRICK SICKELS

INTERNAL AUDITOR

CU*ANSWERS, A CREDIT UNION SERVICE ORGANIZATION

PSICKELS@CUANSWERS.COM

800.327.3478 X335

PROFESSIONAL BACKGROUND

- Internal Auditor for 9 years
- Financial Compliance for 6 years
- Attorney in Michigan
- Member of ISACA

CU*ANSWERS BACKGROUND



- We are a CUSO
- For 45 years has been a data processor (software/technology company)
- Serve over 200 credit union clients
- We are owned by our clients only, with shareholders owning 200 shares and having 1 vote each
- We are looking to push examination innovation and reduce the cost of compliance to our clients
- We also provide IT Support, Compliance Services, and a host of other services in the industry

CU*ANSWERS BACKGROUND

We look for our clients to help us develop software that will help them with their compliance concerns.

https://auditlink.cuanswers.com/wp-content/uploads/AuditLink_Top_Ten.pdf

AuditLink

TOPTEN

3

Critical Field Monitoring

Activity – Currently credit unions must review the file maintenance logs to determine if the changes made to member accounts were completed correctly and with the proper authority.

Solution – Develop a process where the credit union can choose critical system fields to be displayed separately on the file maintenance log. At the end of the day, populate a screen similar to the one used for BSA daily monitoring where the credit union would work these changes in real time.

Status – *In process: Project sheet #33097 is assigned to a programmer and is currently being worked on.*

POLICY **VERSUS** PROCEDURE

1. Your policy should be a **rule**. “You must use encryption to send emails with sensitive information.”
2. Your procedure should be the **how**. You sign into MOVEIT, use Zix, etc.

Encryption of Sensitive Information

Users who send or receive sensitive information via electronic communications are required to use encryption when this information is sent out beyond the CU*Answers network borders (such as external email recipients).

“EFFECTIVENESS”

Cybersecurity presents a unique problem. We can measure whether a financial institution is healthy or not through measurement of ratios, capitalization, and so forth.

The purpose of cybersecurity is to avoid loss, both tangibly and intangibly. An example of intangibility is **reputation risk**.

Therefore, the best result is **zero**. Unfortunately, IT lives in a realm where “zero” is usually the last place of objectivity. Most everything else is subjective – “is the credit union’s IT controls commensurate with the risk?” Loaded question you see **everywhere**.

“EFFECTIVENESS”

However, a result of **zero** doesn't necessarily mean that policies and procedures in place are effective. (Not a bad idea to get some background on what “zero” actually means).

Sony, Target, Office of Personnel Management may have all thought they were “effective.”

Until they weren't.

http://www.amazon.com/Zero-The-Biography-Dangerous-Idea/dp/0140296476/ref=pd_sim_14_1?ie=UTF8&refRID=1JAT8NHTWTTG99WVE8D4

“EFFECTIVENESS”

So when a financial institution is writing a policy, or an examiner is reviewing the policy, we should try to think of what the **measurable, end goals** might be.

<https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/five-most-common-cyber-security-mistakes.PDF>



DEFINITIONS

“Our goal should be 100% security.”

100% security is not feasible nor appropriate.

Instead: Policies and procedures should be “business as usual.”

“Security is dependent on ‘best of breed’ technology.”

Effective security is less dependent on technology.

Instead: “How can we adapt the human behavior to maximize our technology investment?”

“Our defenses need to exceed the tools of the hackers.”

Advancement in technology can always disrupt your defenses, making the arms race unwinnable.

Instead: What do we value, and how can we best protect that information?

EXAMPLE OF LOSING THE TOOLS ARMS RACE

In 2015, an Italian firm that sold hacking tools was hacked itself, and the documents revealed how it did business with repressive regimes:

In response to concerns that **Hacking Team supplied tools to repressive states which could be used to hack into and spy on almost anyone**, Vincenzetti said: “We did [sell tools to **Libya**] when suddenly it seemed that the Libyans had become our best friends.” **He also admitted providing tools to Egypt, Ethiopia, Morocco and Sudan**, as exposed by the company’s email archive, though denied dealing with Syria.

But Vincenzetti said: “The geopolitical changes rapidly, and sometimes situations evolve. But we do not trade in weapons, we do not sell guns that can be used for years.” He said that without regular updates its tools are rapidly blocked by cyber security countermeasures.

In the case of **the Ethiopian** government, which used Hacking Team tools to spy on journalists and activists, Vincenzetti said: “**We’re the good guys** ... when we heard that Galileo had been used to spy on a journalist in opposition of the government, we asked about this, **and finally decided to stop supplying them in 2014.**”

<http://www.theguardian.com/technology/2015/jul/13/hacking-team-ethiopia-attack-data>

DEFINITION

“Compliance is about monitoring.”

Compliance is about learning.

Instead: What lessons have we learned, and how will we apply these in the future?

Real life example: CU*Answers took a third party service offline that might have had a vulnerability. Some clients were angry about this and wanted the service restored. But we would be turning it on for **everyone**.

We will never turn on a service until all clients using the service have agreed to accept the risk.

Recommendation

*CU*Answers should **never** restore services that may be vulnerable until we have approval from a credit union officer authorized to do so, and should **never** restore services until **all** affected credit unions agree to release CU*Answers from liability.*

*** Protocol**

For Responding to
Cyber Security
Vulnerabilities

DEFINITION

“We need professionals to defend ourselves.”

Security is an attitude, not a department.

Instead: How can we make security everyone’s responsibility?

What sort of rewards do you provide for enforcing security? What sort of punishments?

For example, our CEO is known to walk through the building without ID and reward people on the spot for calling him out on it.

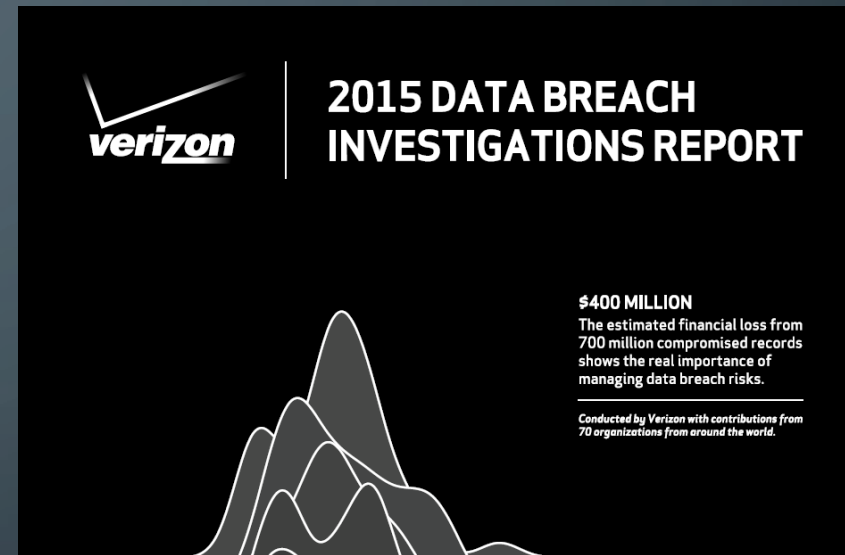
Conversely, when people make mistakes we want them to tell us. An employee has an **incentive to lie or hide** the mistake if they will be fired for it.

WHAT DOES THE DATA TELL US?

There are three main categories of attack vectors:

1. External
2. Internal
3. Partner or client

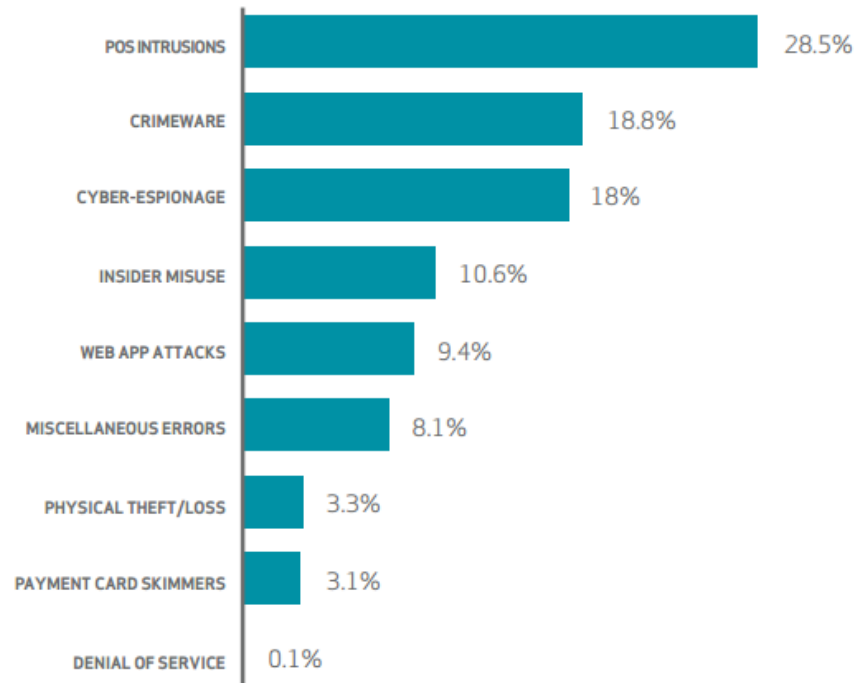
Your policies should cover all of these possibilities.



<http://www.verizonenterprise.com/DBIR/2015/>

WHAT DOES THE DATA TELL US?

There are a few interesting things to note about the breakdown of incident patterns. Let's start with Figure 24, which addresses all security incidents reported for 2014. It may not be obvious at first glance, but the common denominator across the top four patterns—accounting for nearly 90% of all incidents—is people. Whether it's goofing up, getting infected, behaving badly, or losing stuff, most incidents fall in the PEBKAC and ID-10T über-patterns. At this point, take your index finger, place it on your chest, and repeat "I am the problem," as long as it takes to believe it. Good—the first step to recovery is admitting the problem.



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

\$400 MILLION
The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

WHAT DOES THE DATA TELL US?

The Australian Government has a pretty good list of all the different cybersecurity mitigation strategies. This can be a handy reference for reviewing what policies you need. You may agree or disagree with the conclusions but the list itself as reference is valuable.

- 5. While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 strategies remains very high. At least 85% of the cyber intrusions that ASD responds to involve adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.
- 6. Implementing the Top 4 mitigation strategies can be achieved gradually, firstly on workstations of users who are most likely to be targeted by cyber intrusions, and then implementing them on all workstations and servers. Once this is achieved, organisations can selectively implement additional mitigation strategies to address security gaps until an acceptable level of residual risk is reached.

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

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)	Mitigation Strategy	Overall Security Effectiveness
1 (1)	Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential
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
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
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

BUSINESS AS USUAL

Incorporate as much as possible policy guidelines that help your staff know their responsibilities and do their jobs.

MINIMUM GUIDELINES FOR SECURING SENSITIVE INFORMATION

Sending confidential information to other parties through secure and/or encrypted methods



Reasonable assurance that the recipient of confidential information is authorized to receive the information



Disclosing confidential information only when authorized to do so, and refraining from disclosure if there is any doubt regarding the employees' authority to do so



Notifying the organization through Security Incident Reports when a breach of confidential data is known or suspected



HUMAN ELEMENT

TOP 10 THINGS TO KNOW ABOUT SECURITY AT CU*ANSWERS

IF YOU BELIEVE YOU HAVE BEEN COMPROMISED, CHANGE YOUR PASSPHRASE IMMEDIATELY: Everyone has the potential to be the victim of a social engineering attack. If you believe you have been compromised, the first thing to do is change your password. Immediately changing your password can prevent an attack. Do this even before contacting the help desk at x266.

Use **direct communication** to help employees understand their responsibilities.

Testing these responsibilities through internal penetration or social engineering tests can be very valuable. If your employees don't understand, consider redrafting the policy!

VALUE

Provide practical advice to employees on what they need to protect.

Invest in protecting the areas that are identified by the policy.

SENSITIVE INFORMATION

*Sensitive information includes trade secrets, confidential or proprietary information of CU*Answers, its partners or clients, and the non-public personally identifiable financial information of credit union consumers or members, as well as the employees and contractors of CU*Answers.*

It is a **violation** of this policy to:

*Send sensitive information in clear text to a recipient outside of the CU*Answers network;*

Store sensitive information on Public network drives or other electronic storage that lacks user access controls;

Save sensitive information to local hard drives;

Dispose of sensitive information in an insecure manner (e.g. not using shred bins for paper documents); or

Transmit or deliver sensitive information to parties outside the organization in an insecure manner.

These controls shall be reviewed on an ongoing basis; the review of electronic storage controls shall be done on no less than an annual basis.

LESSONS LEARNED

Update policies and procedures as technology changes.

Make sure changes are communicated.

Ensure there is a review of policies. Give someone a **bonus** if you have to. But there is no more effective way of defusing problems by saying something bad happened – **but we learned from it.**

By contrast, the worst thing you can do is have something bad happen and then have the same bad thing happen because you made no changes. This is where **class action lawsuits** are born.

Consent to Remote Wipe

All Users must consent to have their mobile access device, whether personal or CU*Answers issued, remotely wiped in the case of termination of employment, loss of the device, or suspicion of a security breach. CU*Answers is not responsible for any loss of personal information which may be stored on the device.

ATTITUDE

Use your auditors. Your auditors need be less in the “write people up” business, and more in the **continuous improvement** business.

It may not be the people that are the problem. It may be the policy or the procedure that is at issue.

EXAMINATION PROTOCOL

*This document is intended to establish general guidelines for any agency, individual or audit firm performing an audit or regulatory exam at CU*Answers. This protocol is intended to streamline the audit process, ensure that all appropriate individuals are involved from the outset of the audit/review, reduce the overall time associated with the process, and assure that any audit findings are based on correct information.*

If any procedures outlined result in significant burden on behalf of any department being reviewed or on the external audit firm or agency, the Internal Audit department will work with the department or auditor to modify this protocol as necessary.

FFIEC REVIEW



FFIEC CYBERSECURITY ASSESSMENT
GENERAL OBSERVATIONS

So now that we have a an idea on what our policies look like, what should effective policies be **about?**

Fortunately, the FFIEC has provided some valuable cybersecurity information that gives and overview of what a financial institution should have covered.

1. CYBERSECURITY INHERENT RISK: Connections, services, and technologies used.

http://www.ncua.gov/Resources/CUs/Documents/FFIEC_Cybersecurity_Assessment_Observations.pdf

FFIEC REVIEW

2. CYBERSECURITY PREPAREDNESS: Risk Assessments, collaboration, controls, review and governance, vendor management, and disaster recovery (or resilience).

Chances are, most credit unions will already have some or all of these policies in place at some level with respect to Information Technology. Our recommendation is that you repackage these policies and procedures with a new **cybersecurity** heading and follow the general organization laid out by the NCUA.

The questions posed here are pretty good and your policies should allow you to answer these questions. You know you are in good shape when you can answer these effectively.

Questions to Consider

- In the event of a cyber attack, how will our financial institution respond internally and with customers, third parties, regulators, and law enforcement?
- How are cyber incident scenarios incorporated in our financial institution's business continuity and disaster recovery plans? Have these plans been tested?

GOVERNANCE

While in general the NCUA's document is pretty good, I do believe this statement about **routinely** discussing cybersecurity is rather naive.

Credit union boards are **volunteer**, many of whom do not have an information technology background.

Risk Management and Oversight

Risk management and oversight involves governance, allocation of resources, and training and awareness of employees.

Many boards discuss cybersecurity with management when cyber attacks are widely reported or when the financial institution experiences an attack. Financial institutions generally leverage existing information security policies and practices to address cybersecurity risks. Routinely discussing cybersecurity issues in board and senior management meetings will help the financial institution set the tone from the top and build a security culture. Strong governance includes clearly defined roles and responsibilities that assign accountability to identify, assess, and manage cybersecurity risks across the financial institution.

GOVERNANCE

Our suggestion is to provide simple updates in the board report that includes cybersecurity updates, such as those provided by vendors.

This allows the information technology information to seep into the board discussions and allows the board to ask questions and look for updates on cybersecurity.

http://www.cuanswers.com/news/Cybersecurity_2014_FINAL.pdf

SAMPLE CYBERSECURITY REPORT

Third Quarter 2014

KEY SECURITY EVENTS

Morbi condimentum non leo vitae cursus. Maecenas sit amet lorem bibendum, pellentesque felis at, vehicula orci. Vivamus vehicula, est sit amet commodo laoreet, lorem tortor varius dolor, at volutpat nulla urna vel urna. Nulla aliquet enim suscipit augue pharetra ultricies. Mauris fringilla tellus elit, id vehicula urna luctus in. Sed in libero mi. Nunc sagittis justo eget lacinia tincidunt. Proin ultrices dui eleifend, varius odio sit amet, consectetur urna.

SECURITY UPDATES

All Firefox users upgraded to Firefox 31, per the US-CERT bulletin of July 22, 2014.

Praesent pharetra justo in odio mollis bibendum. Nam libero lacus, hendrerit ut sem vel, fermentum mollis purus. Proin a elit et nulla fringilla luctus. Donec commodo erat metus, id egestas diam vestibulum quis. Etiam sed suscipit felis. Nullam elementum nibh vitae bibendum dictum. Aliquam dapibus in felis sed suscipit.

WEBSITE HOSTED BY CU*ANSWERS NOT VULNERABLE TO HEARTBLEED

CU*Answers confirmed by website that the credit union's hosted website is not vulnerable to the Heartbleed exploit.

GOVERNANCE

We also suggest building a biographical database of the various people in responsible for information technology and cybersecurity at the organization.

KEY IT/COMPLIANCE BIOGRAPHIES

JODY KARNES, CIO



The Director of Technical Resources for CU*Answers since 1994, Jody Karnes has over 20 years of financial product development experience working with thrift and credit union on-line and in-house products. Prior to coming to CU*Answers in 1994, Ms. Karnes served as the Assistant Vice President of Systems and Programming at Fiserv/Spokane,

DAVE WORDHOUSE



For over 12 years David has served in the credit union industry, architecting and implementing network infrastructure and security solutions for CU*Answers, a Credit Union Service Organization, as well as individual credit unions. As Vice President of Network Technologies, David directs a team of nearly 40 information technology professionals

http://www.cuanswers.com/news/Cybersecurity_2014_FINAL.pdf

FFIEC: RISK PROFILE

FFIEC Cybersecurity Assessment Tool User's Guide

User's Guide

Figure 1: Inherent Risk Profile Layout

Risk Levels

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
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)
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)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

Activity, Service, or Product

The FFIEC did a really good thing, and one terrible thing.

The good is there is a relatively easy to understand profile layout. This can help you develop your policies more effectively. Review and ask “Do we have this? If so, do we have a policy around the security of the item?”

[https://www.ffiec.gov/pdf/cybersecurity/FFIEC CAT User Guide June 2015 PDF2 a.pdf](https://www.ffiec.gov/pdf/cybersecurity/FFIEC%20CAT%20User%20Guide%20June%202015%20PDF2%20a.pdf)

FFIEC: RISK PROFILE

FFIEC Cybersecurity Assessment Tool User's Guide

User's Guide

Figure 1: Inherent Risk Profile Layout

Risk Levels

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
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)
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)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

Activity, Service, or Product

Is it rigid and arbitrary? To an extent. Why does the magic number 11 unsecured connections make my risk Moderate rather than Minimal? As long as I have just 10, I get a much nicer label.

FFIEC: RISK PROFILE

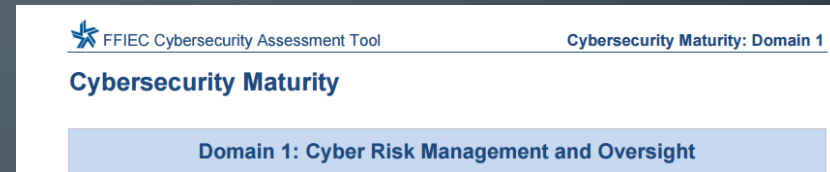
Why would you combine items such as DDoS and phishing attacks? They have an entirely different attack profile and response to just lump them in together.

Category: External Threats	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Attempted cyber attacks	No attempted attacks or reconnaissance	Few attempts monthly (<100); may have had generic phishing campaigns received by employees and customers	Several attempts monthly (100– 500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year	Significant number of attempts monthly (501–100,000); spear phishing campaigns targeting high net worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple attempted DDoS attacks within the last year	Substantial number of attempts monthly (> 100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks

However, this is not the bigger sin of the FFIEC ...

FFIEC TOOLS: MATURITY MODELS

I believe that the use of maturity models is a mistake.



The FFIEC states in the Guide that:

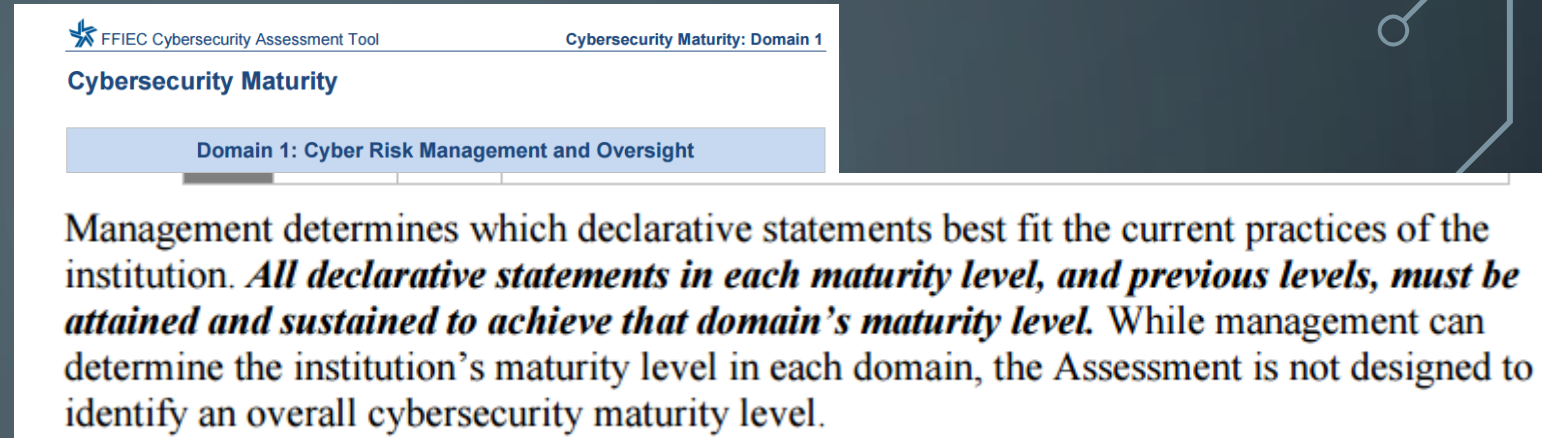
By reviewing both the institution's inherent risk profile and maturity levels across the domains, management can determine **whether its maturity levels are appropriate in relation to its risk**. If not, the institution may take action either to reduce the level of risk or to increase the levels of maturity. **This process is intended to complement**, not replace, an institution's risk management process and cybersecurity program.

[https://www.ffiec.gov/pdf/cybersecurity/FFIEC CAT CS Maturity June 2015 PDF2 c.pdf](https://www.ffiec.gov/pdf/cybersecurity/FFIEC%20CAT%20CS%20Maturity%20June%202015%20PDF2%20c.pdf)

FFIEC TOOLS: MATURITY MODELS

Problems with maturity models:

1. Low-level maturity is not used as a measuring tool in commensurate with the risk being run; rather its used to berate the organization. After all, “immature” is no compliment. It becomes a value judgement rather than objective appraisal of the organization. You can be at a low level of maturity and still be successful at commonly accepted measures.
2. Also note that the FFIEC Guide says you have to meet all levels to reach the next level of maturity. Miss any one, and you are not at that level of maturity. That implies that the organization is not doing something correctly – even if there’s a good reason why management isn’t following a particular requirement.



FFIEC Cybersecurity Assessment Tool Cybersecurity Maturity: Domain 1

Cybersecurity Maturity

Domain 1: Cyber Risk Management and Oversight

Management determines which declarative statements best fit the current practices of the institution. ***All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain’s maturity level.*** While management can determine the institution’s maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.

FFIEC TOOLS: MATURITY MODELS

Problems with maturity models:

3. Maturity is very dependent on **context**. Context changes regularly, however, due to changes in people, technology, and as a result of experimentation and innovation. Trying to define maturity as an objective standard is doomed to fail.

A process model, in and of itself, has no experience.

4. The factors assessed in the FFIEC Guide are **subjective**. This turns maturity from an objective tool to subjective propaganda. For example, should “repeatability” really be something that should be celebrated?

FFIEC TOOLS: MATURITY MODELS

This section is has problems:

1. For example, documented processes don't "consider." **People** consider. This is not just being pedantic. People need guidance on what to do.
2. What does it mean to proactively manage end of life to limit security risks?

Evolving	<p>The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.</p> <p>The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.</p> <p>The institution proactively manages system EOL (e.g., replacement) to limit security risks.</p>
-----------------	---

FFIEC TOOLS: MATURITY MODELS

I don't believe credit union policies should ignore maturity completely, especially because this chart looms over everything. But remember, the core is the following sentence: if **management determines** maturity levels are not appropriate.

You need your audit team to evaluate this and then have management determine if low maturity is a problem.

If your management team does not make the determination, someone else might.

Table 3: Risk/Maturity Relationship

		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				■	■
	Advanced			■	■	■
	Intermediate		■	■	■	
	Evolving	■	■	■		
	Baseline	■	■			

If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels. This process includes

FFIEC TOOLS: MATURITY MODELS

I'm not the only one of this opinion:

[https://www.fsisac.com/sites/default/files/news/FSSCC%20FFIEC%20Cybersecurity%20Assessment%20Comment%20Letter%20\(FR%202015-17907\).pdf](https://www.fsisac.com/sites/default/files/news/FSSCC%20FFIEC%20Cybersecurity%20Assessment%20Comment%20Letter%20(FR%202015-17907).pdf)

<http://www.cujournal.com/news/compliance/why-credit-unions-fear-regulators-new-cybersecurity-tool-1025128-1.html>

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

SUMMARY

Your effective cybersecurity policies and processes whenever possible:

1. Should use plain language that incorporates cybersecurity policies into everyday routine;
2. Should be tested and taught to employees on a regular basis;
3. Should clearly identify what you are trying to protect;
4. Should incorporate lessons learned from experiences;
5. Should be reviewable with an eye toward improving your security, the work it takes to improve the security, or both;
6. Should reference core elements of the FFIEC guidance.

TOOLS: POLICY SWAP

The logo for PolicySwap CUANSWERS is displayed in white text on a dark teal rectangular background. The word "PolicySwap" is in a large, serif font, and "CUANSWERS" is in a smaller, sans-serif font below it.

PolicySwap is where credit unions can go to find or leave policies in use by their peers. You do not need to be in our network to use this tool.

These policies are vetted and reviewed by our Compliance Team for quality assurance.

<http://policyswap.cuanswers.com/>

TOOLS: POLICY SWAP

<input type="checkbox"/>	★	✗	📄	Honor Credit Union	Workout/TDR Checklist Proce	Financial Transaction
<input type="checkbox"/>	★	✓	📄	Delta County Credit Union	Fair Housing Act Policy	Consumer Protection

TOOLS: COST OF COMPLIANCE

For two straight years, we've asked credit unions to submit templates for calculating their costs of compliance.

The goal is not only to derive and display costs, but to associate them with the overall profitability of the credit union.

Industry leaders know these costs are soaring but when asked have no idea what the actual dollar amount of the expense is.

The CU*Answers network started this initiative to begin to understand these costs and their effects on credit union profitability.”

<https://auditlink.cuanswers.com/winners-of-the-second-cost-of-compliance-announced/>

TOOLS: COST OF COMPLIANCE

E) A CU*Answers System Programming Proposal Revisited

You may recall from our initial Cost of Compliance contest submission that we have developed an additional proposal for utilizing the system to track a credit union's compliance costs, albeit one which would require some additional system programming. We reiterate that CU*Answers would need to decide if it is feasible from a cost-benefit standpoint to commit resources to developing the programming, and subsequently including it in a future system upgrade. That would most likely be determined by the costs involved, and the amount of client credit unions that would be motivated enough to utilize it in order to measure their compliance costs. As a client credit union, we felt it was worth putting forth yet again.

Our proposal is as follows, illustrated by accompanying "screen shot" exhibits:

- 1) Add a compliance flag (or checkbox) to each G/L entry line on the MNGELE # 1 screen. Along with the checkbox, there would need to be two radio buttons, one of which is to be clicked if the flag is activated: one designated as "\$" (which would indicate that a certain set dollar amount of the G/L entry is to be designated as a compliance cost), and one designated as "%" (which would indicate that a certain percentage of the G/L entry is to be designated as a compliance cost). The final box would allow the entry of a set dollar amount, or a percentage, depending upon which radio button was clicked. Please refer to Exhibit 1.
- 2) The same methodology would be utilized on the MNACCK # 1 screen. This covers the compliance cost of items which are paid by check, without creating the need for any more multiple G/L entries to be used other than to cover the range of expenses for the invoice. Please refer to Exhibit 2.

TOOLS: CYBERSECURITY FOR CREDIT UNION BOARDS



TOOLS: CYBERSECURITY FOR CREDIT UNION BOARDS

Free to the industry

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

Video for credit union directors on cybersecurity basics

Policy Templates

Risk Assessments

FFIEC and NCUA Resources

Coming soon: Audit plans for cybersecurity

A decorative graphic on the left side of the slide, consisting of white lines and circles on a dark blue background, resembling a circuit board or a network diagram.

THANK YOU

PATRICK SICKELS

CU*ANSWERS

PSICKELS@CUANSWERS.COM

800.327.3478 X335