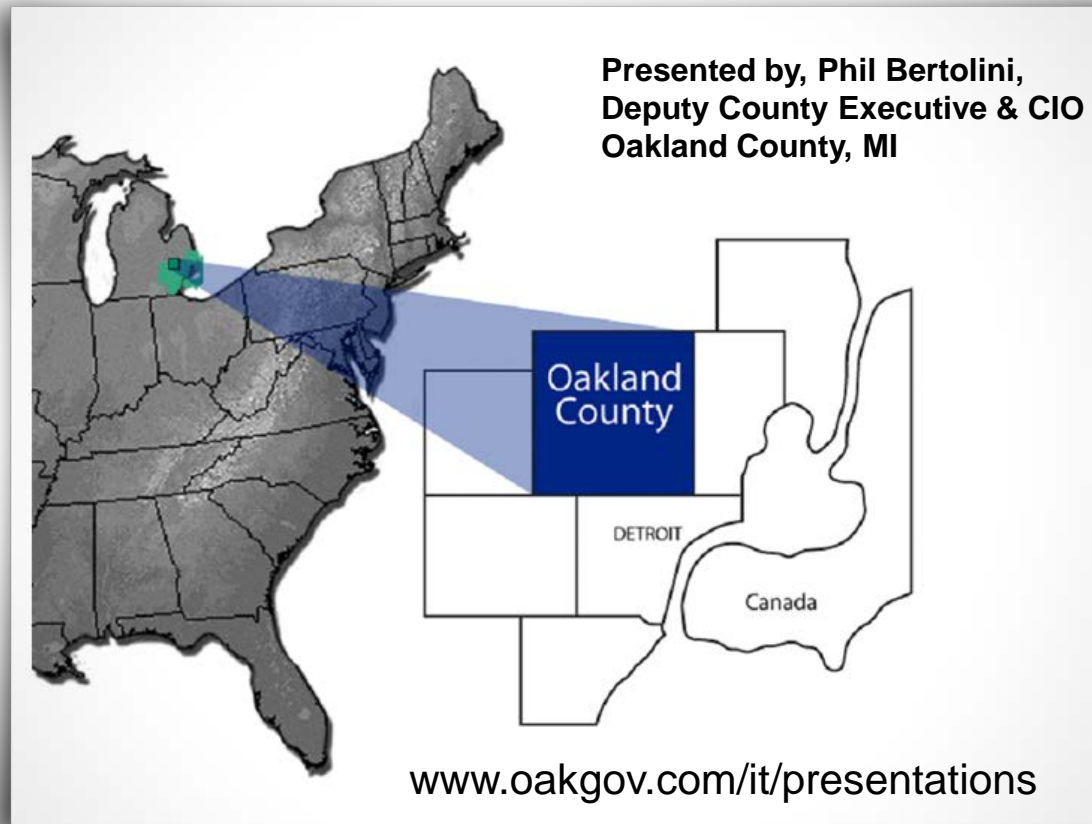


What Finance Officers Need to Know About Cyber Security



February 2015

Agenda

- **Introduction**
- **Business Challenge**
- **Technical Challenge**
- **CySAFE**
- **Recommendations**

Massive breach at health care company Anthem Inc.



Elizabeth Weise, USATODAY

9:26 a.m. EST February 5, 2015



Security breach affects personal information of city employees, Detroit says

8:31 AM, March 3, 2014 | 1 Comments

Recommend 12 people recommend this. Sign up to see what your friends recommend.

Recommend 12

Tweet 0

+1 2

Pin it

Print Email Share

Associated Press

FILED UNDER

Local News

City Of Detroit

Detroit says a recent computer security breach affected files that contained personal identifying information of a large number of city employees.

The city says in a statement that Beth Niblock, Detroit's chief information officer, plans to discuss the breach during a Monday



AP The Associated Press @AP

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

2,894 RETWEETS

134 FAVORITES



10:07 AM - 23 Apr 13



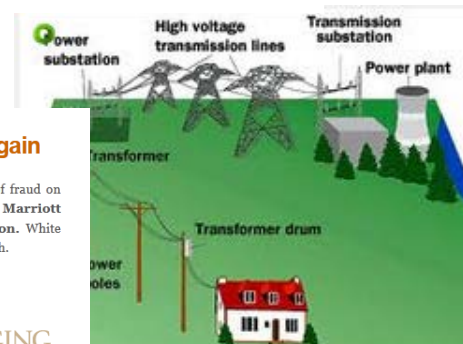
Data Breaches — 34 comments

03 Banks: Card Thieves Hit White Lodging Again

For the second time in a year, multiple financial institutions are complaining of fraud on customer credit and debit cards that were all recently used at a string of Marriott properties run by hotel franchise firm White Lodging Services Corporation. White Lodging says it is investigating, but that so far it has found no signs of a new breach.

In January 31, 2014, this author first reported evidence of a breach at some White Lodging locations. The Merrillville, Ind. based company confirmed a breach three days later, saying hackers had installed malicious software on cash registers in food and beverage outlets at 14 locations nationwide, and that the intruders had been stealing customer card data from these outlets for approximately nine months.

WHITE LODGING



Agenda

- Introduction
- **Business Challenge**
- Technical Challenge
- CySAFE
- Recommendations

Business Challenges

- How to get started with a cybersecurity initiative?
- How to prioritize efforts?
- How to gauge impact / risk of needs?
- How to measure results and progress?

Cyber Security

KEEP IT SIMPLE

Cyber Security

**KEEP IT
CLEAR**

Cyber Security





Agenda

- Introduction
- Business Challenge
- **Technical Challenge**
- CySAFE
- Recommendations

[illegible]

10 Worst Data Breaches of All Time

By Elizabeth Palermo SEPTEMBER 21, 2014 11:06 AM - Source: Tom's Guide US |  0 COMMENT

TAGS : [Security](#)  [Privacy](#) 



Credit: Milos Stojanovic/Shutterstock

Technical Challenge

- Numerous cybersecurity standards exist



International
Organization for
Standardization



Minimizing Time, Cost, and Risk

While Maximizing Control and Meeting Compliance Standards







Framework for Improving Critical Infrastructure Cybersecurity



Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Developed by NIST under a Presidential initiative

Targeted for government

39 Pages of summary and references to other frameworks

98 Controls

Category	Subcategory	Informative References
Asset Management (IDAM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID-AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none">CCS CSC 1COBIT 5 BAI09.01, BAI09.02ISA 62443-2-1:2009 4.2.3.4ISA 62443-3-3:2013 SR 7.8ISO/IEC 27001:2013 A.8.1.1, A.8.1.2NIST SP 800-53 Rev. 4 CM-8
	ID-AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none">CCS CSC 2COBIT 5 BAI09.01, BAI09.02, BAI09.05ISA 62443-2-1:2009 4.2.3.4ISA 62443-3-3:2013 SR 7.8ISO/IEC 27001:2013 A.8.1.1, A.8.1.2NIST SP 800-53 Rev. 4 CM-8
	ID-AM-3: Organizational communication and data flows are mapped	<ul style="list-style-type: none">CCS CSC 1COBIT 5 DSS05.02ISA 62443-2-1:2009 4.2.3.4ISO/IEC 27001:2013 A.13.2.1NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
	ID-AM-4: External information systems are catalogued	<ul style="list-style-type: none">COBIT 5 APO02.02ISO/IEC 27001:2013 A.11.2.6NIST SP 800-53 Rev. 4 AC-20, SA-9
	ID-AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none">COBIT 5 APO03.03, APO03.04, BAI09.02ISA 62443-2-1:2009 4.2.3.6ISO/IEC 27001:2013 A.8.2.1NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
	ID-AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none">COBIT 5 APO01.02, DSS06.03ISA 62443-2-1:2009 4.3.2.3.3ISO/IEC 27001:2013 A.6.1.1NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
		<ul style="list-style-type: none">COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05

NIST

NIST
National Institute
of Standards
and Technology

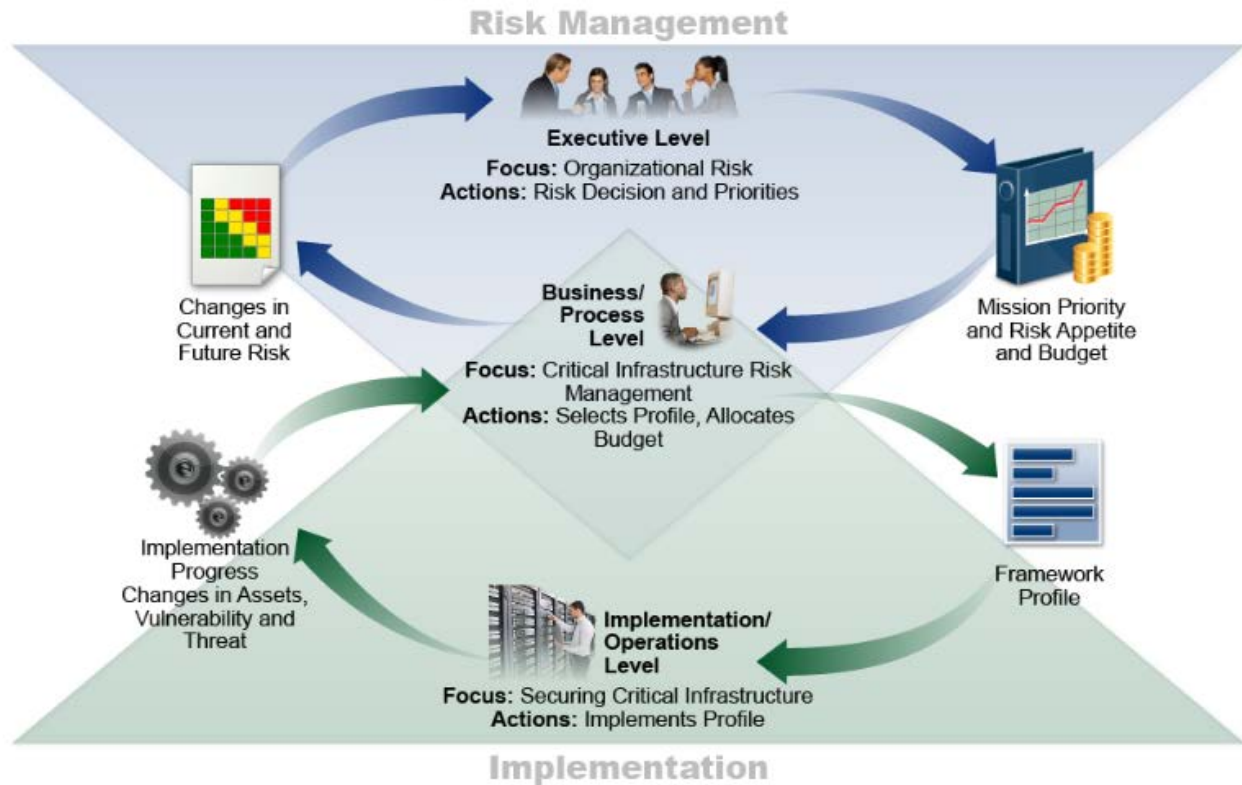


Figure 2: Notional Information and Decision Flows within an Organization

ISO 27000



International
Organization for
Standardization

The **ISO/IEC 27000-series** (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises [information security](#) standards published jointly by the [International Organization for Standardization](#) (ISO) and the [International Electrotechnical Commission](#) (IEC).

The series provides [best practice](#) recommendations on information security management, risks and controls within the context of an overall [information security management system](#) (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

ISO 27000



International
Organization for
Standardization

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues.

It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant.

Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

ISO 27000



International
Organization for
Standardization

ISO27k ref.		Description	Control Total
Management	4	Context of the organization	8
	5	Leadership	19
	6	Planning	39
	7	Support	28
	8	Operation	9
	9	Performance evaluation	29
	10	Improvement	16
ISMS Control Point Total:			148
Operational	A5	Management direction for information security,	2
	A6	Organisation of information security,	7
	A7	Human Resource security,	6
	A8	Asset Management,	10
	A9	Access control,	13
	A10	Cryptography,	2
	A11	Physical and Environmental security,	15
	A12	Operations Security,	14
	A13	Communications Security,	7
	A14	System acquisition, Development and Maintenance,	13
	A15	Supplier Relationships,	5
	A16	Information Security Incident Management,	7
	A17	Information Security Aspects of Business Continuity	4
	A18	Compliance	8
Annex 'DIS' Control Objective Total:			113
Total Control Points :			261



20 Critical Controls

Critical Security Controls – Version 5

- [1: Inventory of Authorized and Unauthorized Devices](#)
- [2: Inventory of Authorized and Unauthorized Software](#)
- [3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers](#)
- [4: Continuous Vulnerability Assessment and Remediation](#)
- [5: Malware Defenses](#)
- [6: Application Software Security](#)
- [7: Wireless Access Control](#)
- [8: Data Recovery Capability](#)
- [9: Security Skills Assessment and Appropriate Training to Fill Gaps](#)
- [10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches](#)
- [11: Limitation and Control of Network Ports, Protocols, and Services](#)
- [12: Controlled Use of Administrative Privileges](#)
- [13: Boundary Defense](#)
- [14: Maintenance, Monitoring, and Analysis of Audit Logs](#)
- [15: Controlled Access Based on the Need to Know](#)
- [16: Account Monitoring and Control](#)
- [17: Data Protection](#)
- [18: Incident Response and Management](#)
- [19: Secure Network Engineering](#)
- [20: Penetration Tests and Red Team Exercises](#)

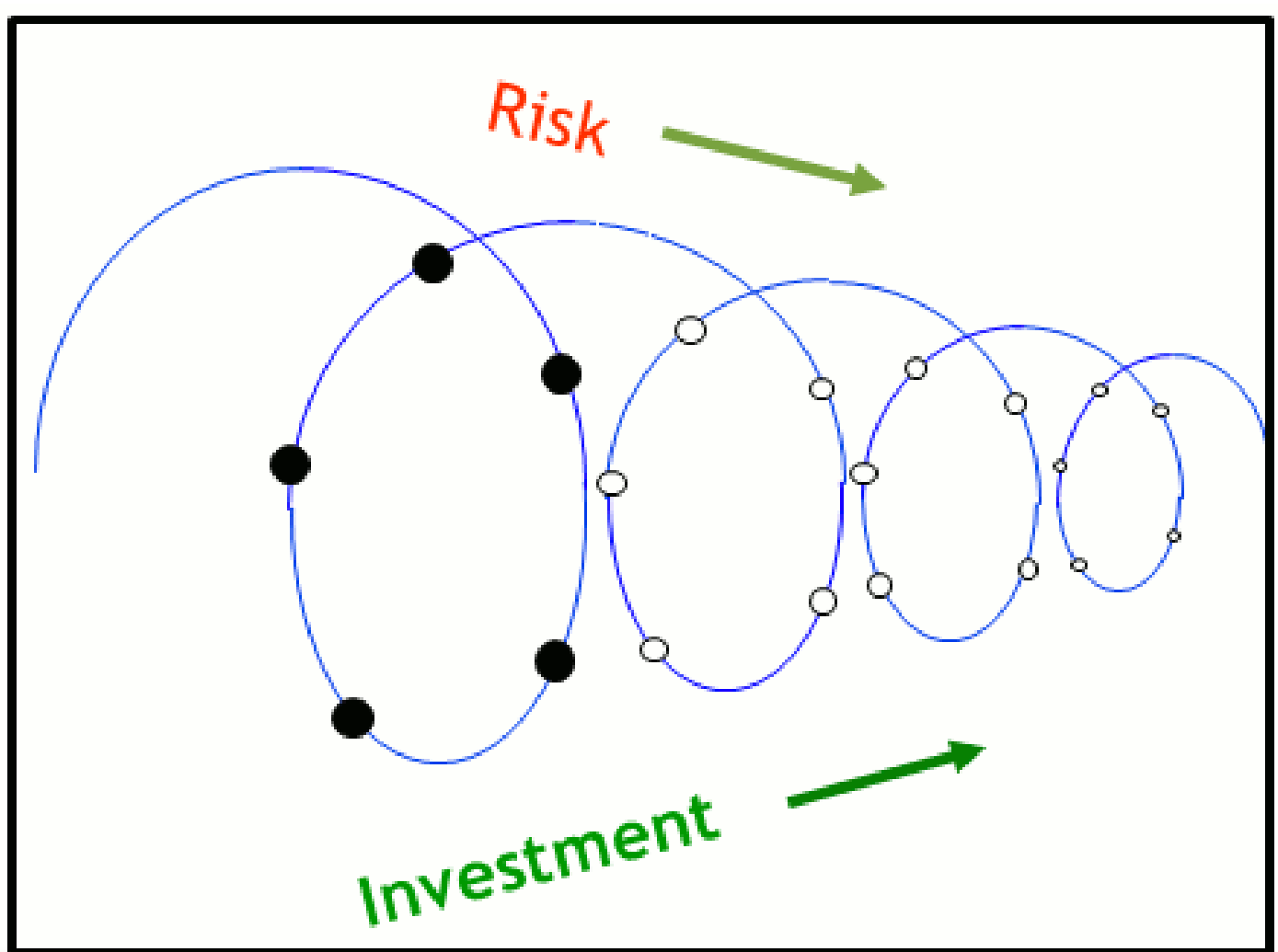


20 Critical Controls

Clear examples of control outputs based on current maturity and end goal

More Technical than Management

Recommend order of implementation debatable



Measuring Risk

What is the Risk Equation?

$\text{Risk} = \text{Impact} \times \text{Probability/Cost}$



Agenda

- Introduction
- Business Challenge
- Technical Challenge
- **CySAFE**
- Recommendations



www.g2gmarket.com

CySAFE Team

- Phil Bertolini, Chris Burrows – Oakland County
- Ed Winfield, Jeff Small – Wayne County
- Andy Brush – Washtenaw County
- Rich Malewicz – Livingston County
- Colleen Hinzmann – Monroe County
- Jessica Moy – State of Michigan



- A practitioner's experience with these standards
- Need an organized approach that addresses IT Security **Management** issues and **Technical** controls
- 95/5 Rule (36 Controls out of 379)
- All controls factor (Cost / Time / Risk)
- Reports built-in with trending and graphs
- Private (only you have the data)
- Takes 60 minutes to complete the assessment
- **FREE**



Overview

In the world of cyber security, local governments often struggle to keep pace with an ever-changing threat environment. CySAFE was created through a collaborative effort, driven by five Michigan counties and the State of Michigan to develop a free IT security assessment tool to help small and mid-sized government agencies assess, understand and prioritize their **basic** IT security needs.

CySAFE was created from three well-known IT security frameworks: 20 Critical Controls, ISO 27001 and NIST. The goal was to combine the 379 controls from all three frameworks into one condensed list, removing any redundant controls and assess the controls against the government agency's current IT security capabilities. Next, the master list of 36 controls were evaluated over three key factors – cost to implement, time to implement and risk – and were assigned a number based on each key factor. The evaluation was completed in a collaborative effort by the IT specialists from the six participating Michigan government agencies (See Appendix).

How to Use CySAFE

Step 1: Understand the Source Frameworks

CySAFE was built upon current industry IT security standards: 20 Critical Controls, ISO 27001 and NIST. For a description of the 36 controls from each framework used with CySAFE, review the worksheets labelled 20 CC, ISO and NIST. This will provide you with an understanding of the recommended IT security controls, descriptions and approaches. For more detailed background information on the security standards documents, refer to the links found in the Appendix worksheet.

Step 2: Become Familiar With the Tool

CySAFE was built in a Microsoft Excel workbook with eight worksheets. Each worksheet plays a different role in evaluating and understanding IT security readiness.

Cyber Security Assessment for Everyone CySAFE EXAMPLE 091014.xlsx - Microsoft Excel

CySAFE

Cyber Security Assessment for Everyone

Assessment

Assessment Rating Scale Legend

0 - Non-Existent Management processes are not recognizable processes. The organization has no processes to be addressed).

1 - Initial Processes are ad hoc and disorganized. The organization has recognized that the issues exist. However, there are no standardized processes tend to be applied on an individual or case-by-case basis (management is disorganized).

2 - Repeatable Processes follow a regular pattern where different people undertaking the same task. There is no formal training or communication responsibility is left to the individual. There is no knowledge of individuals and errors are likely to be repeated.

3 - Defined Processes are documented and standardized and documented and communicated. However, compliance with the procedures is not guaranteed. Deviations will be detected. The procedures are the formalization of existing practice.

4 - Managed Processes are monitored and measured compliance with procedures and tend to be working effectively. Processes are provided good practice. Automation and too many ways).

5 - Optimized Best practices are followed and refined to a level of best practice, based on benchmarking with other organizations in an integrated way to automate the workflow.

Legend

The values assigned to Cost (Column E), Time (Column F), Risk (Column G), Total (Column H), Rating (Column I) and CySAFE Score (Column J) are for five Michigan Counties and the State of Michigan.

Cost (Column E) Time (Column F)
 0 < \$25K 0 < 60 days
 1 \$25K - \$75K 1 61-120 days
 2 > \$75K 2 > 121 days

Framework	Control Name	Cost	Time	Risk	Total	Rating	CySAFE Score
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	3	3	2	8		No Score Yet
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	3	3	2	8		No Score Yet
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	3	3	2	8		No Score Yet
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	3	3	2	8		No Score Yet
20 CC	Critical Control 5: Malware Defenses	3	3	2	8		No Score Yet
20 CC	Critical Control 6: Application Software Security	3	3	2	8		No Score Yet
20 CC	Critical Control 7: Wireless Device Control	3	3	2	8		No Score Yet
20 CC	Critical Control 8: Data Recovery Capability	3	3	2	8		No Score Yet
20 CC	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	3	3	2	8		No Score Yet
20 CC	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	3	3	2	8		No Score Yet
20 CC	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	3	3	2	8		No Score Yet
20 CC	Critical Control 12: Controlled Use of Administrative Privileges	3	3	2	8		No Score Yet
20 CC	Critical Control 13: Boundary Defense	3	3	2	8		No Score Yet
20 CC	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	3	3	2	8		No Score Yet
20 CC	Critical Control 15: Controlled Access Based on the Need to Know	3	3	2	8		No Score Yet
20 CC	Critical Control 16: Account Monitoring and Control	3	3	2	8		No Score Yet
20 CC	Critical Control 17: Data Loss Prevention	2	2	2	6		No Score Yet
20 CC	Critical Control 18: Incident Response and Management	3	3	2	8		No Score Yet
20 CC	Critical Control 19: Secure Network Engineering	1	1	2	4		No Score Yet
ISO	Define Scope	3	3	3	9		No Score Yet
ISO	Setup the Information Security Team and Approach	3	2	3	8		No Score Yet
ISO	Communicate Information Security Policy	3	1	2	6		No Score Yet
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	3	1	2	6		No Score Yet
ISO	Complete Summary of Controls	3	3	3	9		No Score Yet
ISO	Define and Generate Records (evidence)	3	1	1	5		No Score Yet
ISO	Perform Business Management Review (if applicable)	3	1	1	5		No Score Yet
ISO	Conduct Internal ISMS Audits	3	1	3	7		No Score Yet
ISO	Measure Effectiveness of Controls	3	1	2	6		No Score Yet
ISO	Update Annual Planning	3	2	3	8		No Score Yet
ISO	Data Classification (not in the ISMS but valuable)	3	2	3	8		No Score Yet
NIST	Business Environment	3	2	3	8		No Score Yet
NIST	Governance	3	1	2	6		No Score Yet
NIST	Risk Management Strategy	3	1	2	6		No Score Yet
NIST	Maintenance	2	2	3	7		No Score Yet
NIST	Anomalies and Events	3	1	2	6		No Score Yet
NIST	Detection Processes	3	3	3	9		No Score Yet

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.

Basic: Secure configuration
 Change default passwords
 Limit ports/services to only those needed
 Firewall rules



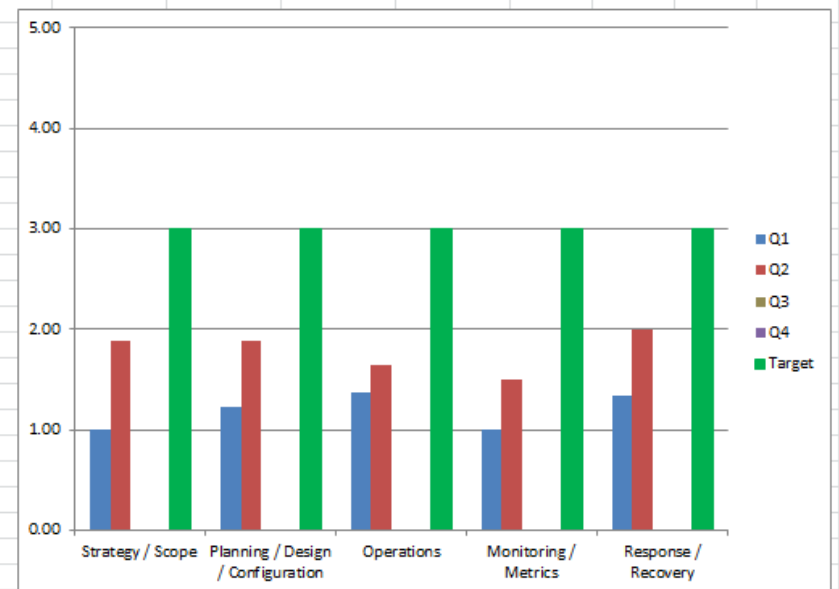
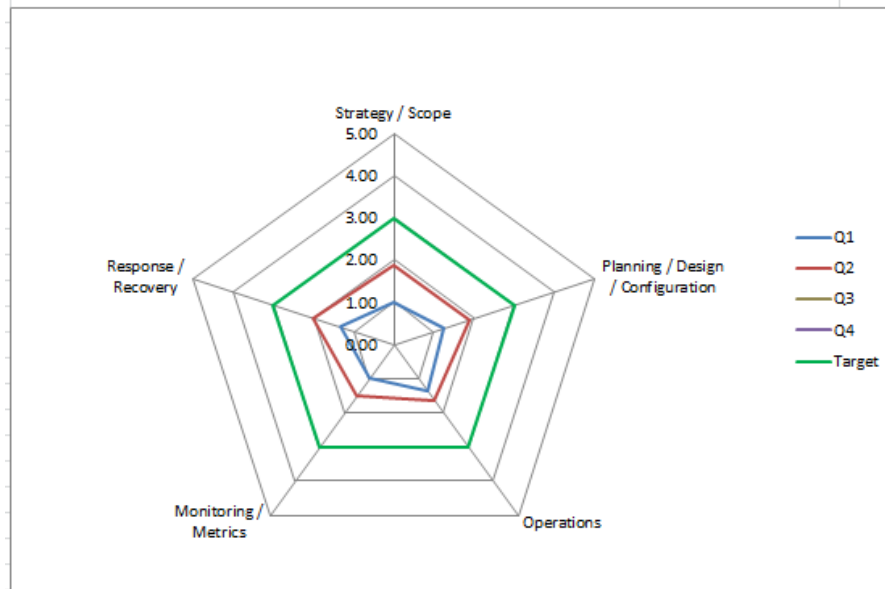
Assessment Results

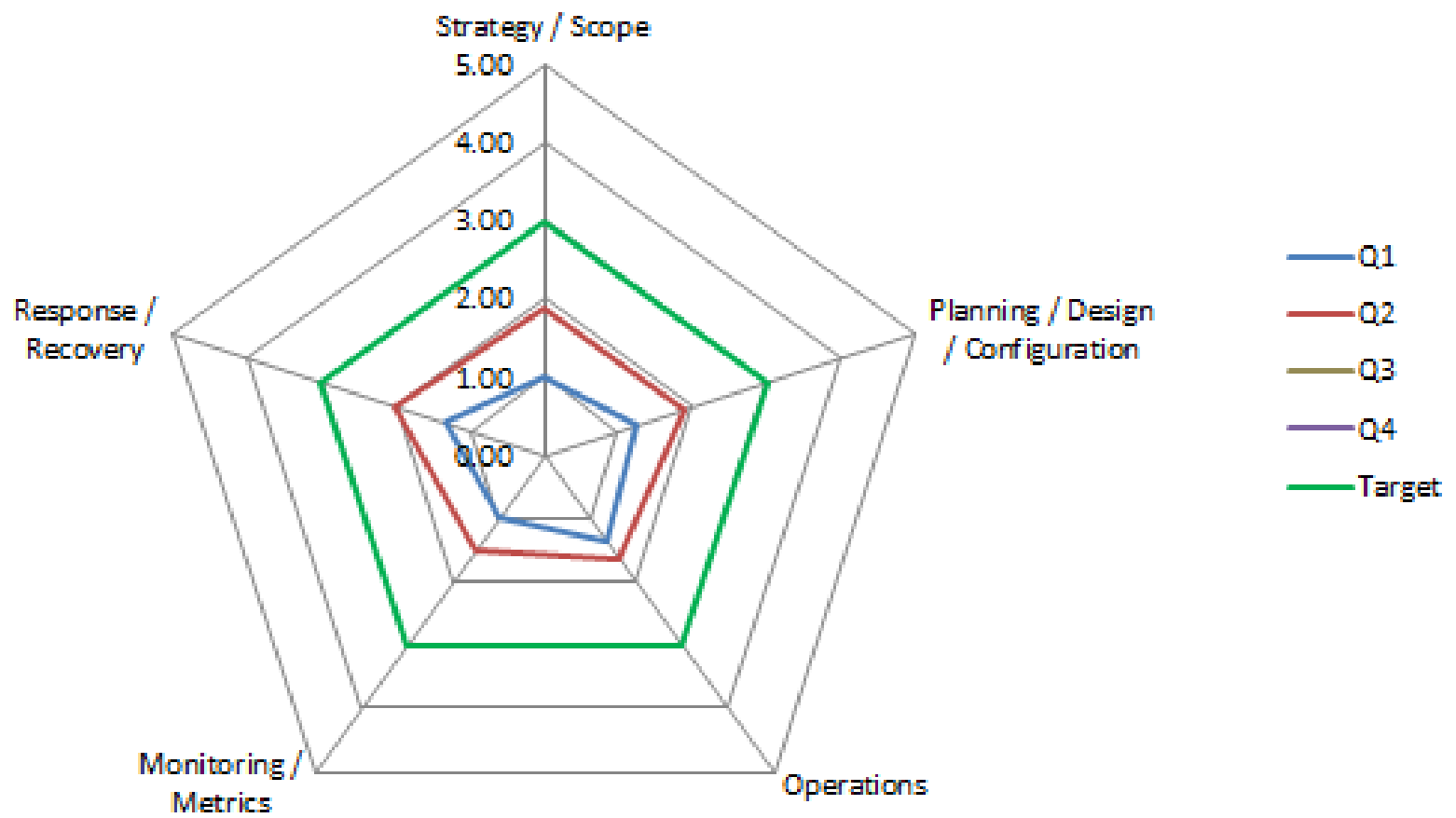
Framework	Control Name	Rating	CySAFE Score
20 CC	Critical Control 12: Controlled Use of Administrative Privileges	0	100
ISO	Complete Summary of Controls	1	85
NIST	Detection Processes	1	85
20 CC	Critical Control 13: Boundary Defense	1	76
ISO	Update Annual Planning	1	76
ISO	Data Classification (not in the ISMS but valuable)	1	76
20 CC	Critical Control 5: Malware Defenses	2	70
ISO	Define Scope	2	70
ISO	Measure Effectiveness of Controls	0	67
20 CC	Critical Control 15: Controlled Access Based on the Need to Know	1	66
NIST	Maintenance	1	66
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	2	62
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	2	62
20 CC	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	2	62
20 CC	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	2	62
20 CC	Critical Control 18: Incident Response and Management	2	62
NIST	Business Environment	2	62
NIST	Governance	1	57
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	2	54
20 CC	Critical Control 8: Data Recovery Capability	2	54
20 CC	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	2	54
20 CC	Critical Control 16: Account Monitoring and Control	2	54
ISO	Conduct Internal ISMS Audits	2	54
20 CC	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	2	47
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	2	47
NIST	Risk Management Strategy	2	47
NIST	Anomalies and Events	2	47
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	3	44
20 CC	Critical Control 7: Wireless Device Control	3	44
ISO	Setup the Information Security Team and Approach	3	44
20 CC	Critical Control 6: Application Software Security	2	39
ISO	Define and Generate Records (evidence)	2	39
ISO	Perform Business Management Review (if applicable)	2	39
20 CC	Critical Control 19: Secure Network Engineering	1	38
20 CC	Critical Control 17: Data Loss Prevention	3	33
ISO	Communicate Information Security Policy	3	33

Control Category and Summary

<i>Category Summary</i>			
Framework	Control Category: Strategy/Scope	Rating	CySAFE Score
ISO	Complete Summary of Controls	1	85
ISO	Update Annual Planning	1	76
ISO	Define Scope	2	70
NIST	Business Environment	2	62
NIST	Governance	1	57
NIST	Risk Management Strategy	2	47
ISO	Setup the Information Security Team and Approach	3	44
ISO	Perform Business Management Review (if applicable)	2	39
ISO	Communicate Information Security Policy	3	33
Average Rating		1.89	
Framework	Control Category: Planning/Design/Configuration	Rating	CySAFE Score
ISO	Data Classification (not in the ISMS but valuable)	1	76
20 CC	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and S	2	62
20 CC	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	2	62
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptop	2	62
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	2	62
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	2	47
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	3	44
20 CC	Critical Control 6: Application Software Security	2	39
20 CC	Critical Control 19: Secure Network Engineering	1	38
Average Rating		1.89	
Framework	Control Category: Operations	Rating	CySAFE Score
20 CC	Critical Control 12: Controlled Use of Administrative Privileges	0	100
NIST	Detection Processes	1	85
20 CC	Critical Control 13: Boundary Defense	1	76
20 CC	Critical Control 5: Malware Defenses	2	70
NIST	Maintenance	1	66
20 CC	Critical Control 15: Controlled Access Based on the Need to Know	1	66
20 CC	Critical Control 16: Account Monitoring and Control	2	54
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	2	54
20 CC	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	2	47
20 CC	Critical Control 7: Wireless Device Control	3	44
20 CC	Critical Control 17: Data Loss Prevention	3	33
Average Rating		1.64	
Framework	Control Category: Monitoring/Metrics	Rating	CySAFE Score
ISO	Measure Effectiveness of Controls	0	67
ISO	Conduct Internal ISMS Audits	2	54
20 CC	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	2	54
ISO	Define and Generate Records (evidence)	2	39
Average Rating		1.50	
Framework	Control Category: Response/Recovery	Rating	CySAFE Score
20 CC	Critical Control 18: Incident Response and Management	2	62
20 CC	Critical Control 8: Data Recovery Capability	2	54
NIST	Anomalies and Events	2	47
Average Rating		2.00	

Control Category	Q1	Q2	Q3	Q4	Target
Strategy / Scope	1.00	1.89			3.0
Planning / Design / Configuration	1.22	1.89			3.0
Operations	1.36	1.64			3.0
Monitoring / Metrics	1.00	1.50			3.0
Response / Recovery	1.33	2.00			3.0





Appendix

Standards Documents:

20 Critical Controls	http://www.sans.org/critical-security-controls
NIST	www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
ISO 27001	www.iso.org/iso/home/standards/management-standards/iso27001.htm

Reference Documents:

NIST SP 800-53 Rev 4	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Verizon Security Report	http://www.verizonenterprise.com/DBIR/
COIN	http://www.countyinnovation.us/
Capability Maturity Model Integration (CMMI)	http://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration
DHS Cyber Security Homepage	http://www.dhs.gov/topic/cybersecurity
DHS Critical Infrastructure Cyber Community C ³ Voluntary Program	http://www.dhs.gov/about-critical-infrastructure-cyber-community-c³-voluntary-program

Summary

- CySAFE tool is an effective way to assess and plan your cybersecurity efforts
- Designed for any size government entity
- In 60 minutes, you have a Priority List and Graphs
- Data is private; Only stored in Excel format
- Built for governments by governments / FREE
- Available for all via G2G Cloud Solutions

<http://www.g2gmarket.com>

- CySAFE for BUSINESS at www.advantageoakland.com

Agenda

- Introduction
- Business Challenge
- Technical Challenge
- CySAFE
- **Recommendations**

Oakland County Initiatives

1. Secure endpoints by removing ADMIN access
2. ITSEC Training
3. Multi-Factor Authentication
4. Create Cyber Incident Response Plan
5. Improving patching life cycle timing

Recommendations

free or low cost

- Removing Admin rights
- Turning on Windows Firewall
- Bitlocker
- Use a VPN (there are very cheap cloud based VPNs with low cost monthly fees) No hardware or administration costs required
- Turn Browser add-ons on like WOT (Web of Trust), HTTPS only
- Use Least Privilege Model
- Communicate with staff about Risks and current threats.
- Ask the users to report suspicious activity/emails
- Patch often
- Use a shredder
- Create a IT Security Policy and communicate it to users
- Add multifactor authentication
- Change Passwords and make them complex
- Use a Password Manager
- Check your backups
- Stay current with Web Browsers (IE and Firefox) and any other systems that touch the internet
- Segment your network

Recommendations

- Hire a CISO
- # 1 priority for entire IT department
- What standard are you measuring against?
 - ISO 27000
 - NIST
 - SANS 20 Critical Controls
- Prepare to react, respond and recover
- Training is key to success
- The world of cyber security has changed
- Use CySAFE!!!

Wrap Up & Take-Aways

Phil Bertolini, Deputy County Executive & CIO
Oakland County, MI
bertolinip@oakgov.com