SC

CYBER

Cybersecurity Strategies for County Government

March 1, 2018

SC CYBER

Cyber Strategies for County Government

Thomas Scott

Cyber Resilience Professional

- CISSP, CISA, PMP, CRISC
- Critical Infrastructure, FEMA COOP Level 1

STATE EMERGENCY FLORIDA SERT RESPONSE TEAM

C-SAFE Cyber-Security Awareness For Everyone

EMERGENCY MANAGEMENT DIVISION S. C. SOUTH CAROLINA

INFRAGARD PARTNERSHIP FOR PROTECTION

SECURE FLORIDA .org

ISACA® Trust in, and value from, information systems

SC INFORMATION SHARING & ANALYSIS CENTER SC-ISAC

acp

CPAC CONTINGENCY PLANNING ASSOCIATION OF THE CAROLINAS

MS-ISAC

What is Cybersecurity?

Understanding And Managing Your Risks

- ELEMENTS OF RISK
- MANAGING YOUR RISKS
  - Identify what information your county stores and uses
  - Determine the value of your information
  - Develop an inventory
  - Understand your threats and vulnerabilities

SAFEGUARDING YOUR INFORMATION

IDENTIFY

Identify and control who has access to your information

Conduct Background Checks

Require individual user accounts for each employee

Create policies and procedures for information security

PROTECT

Limit employee access to data and information..

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

DETECT

Install and update anti-virus, -spyware, and other –malware programs

Maintain and monitor logs

RESPOND

Develop a plan for disasters and information security incidents

RECOVER

Make full backups of important business data/information

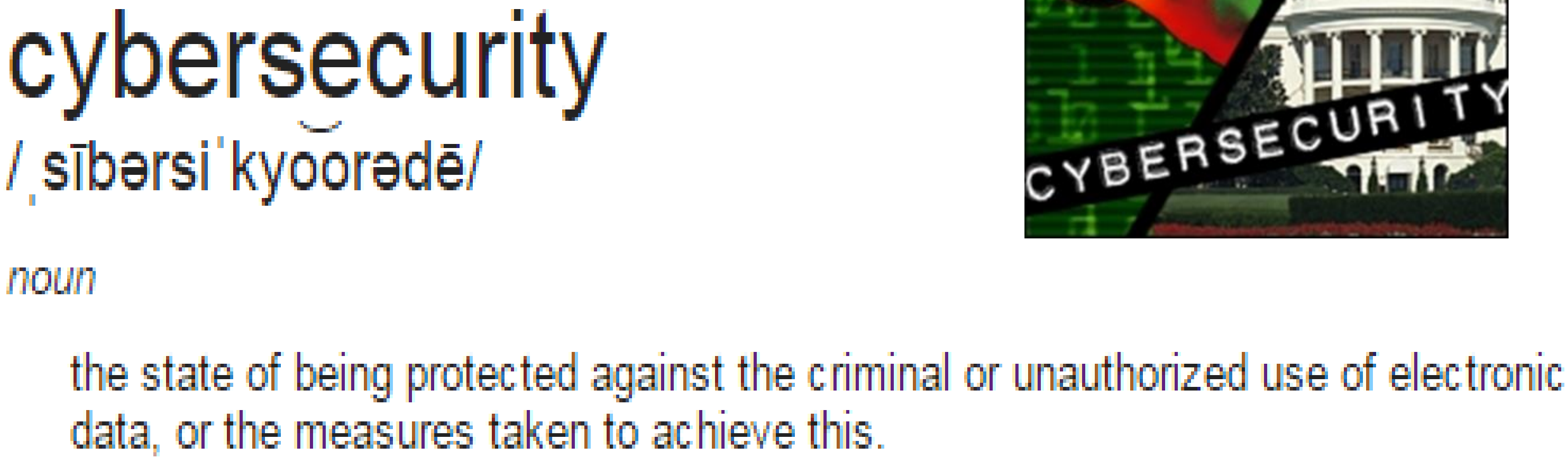
Make incremental backups of important business data/information

Consider cyber insurance

Make improvements to processes / procedures / technologies

SC CYBER

What is Cyber Security?



cybersecurity

/ˌsībərsiˈkyo͝orədē/

noun

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Do you REALLY think the widow of General Sani Obachi wants to share her $8 Million dollars with YOU?

Cyber Threats

Organized crime

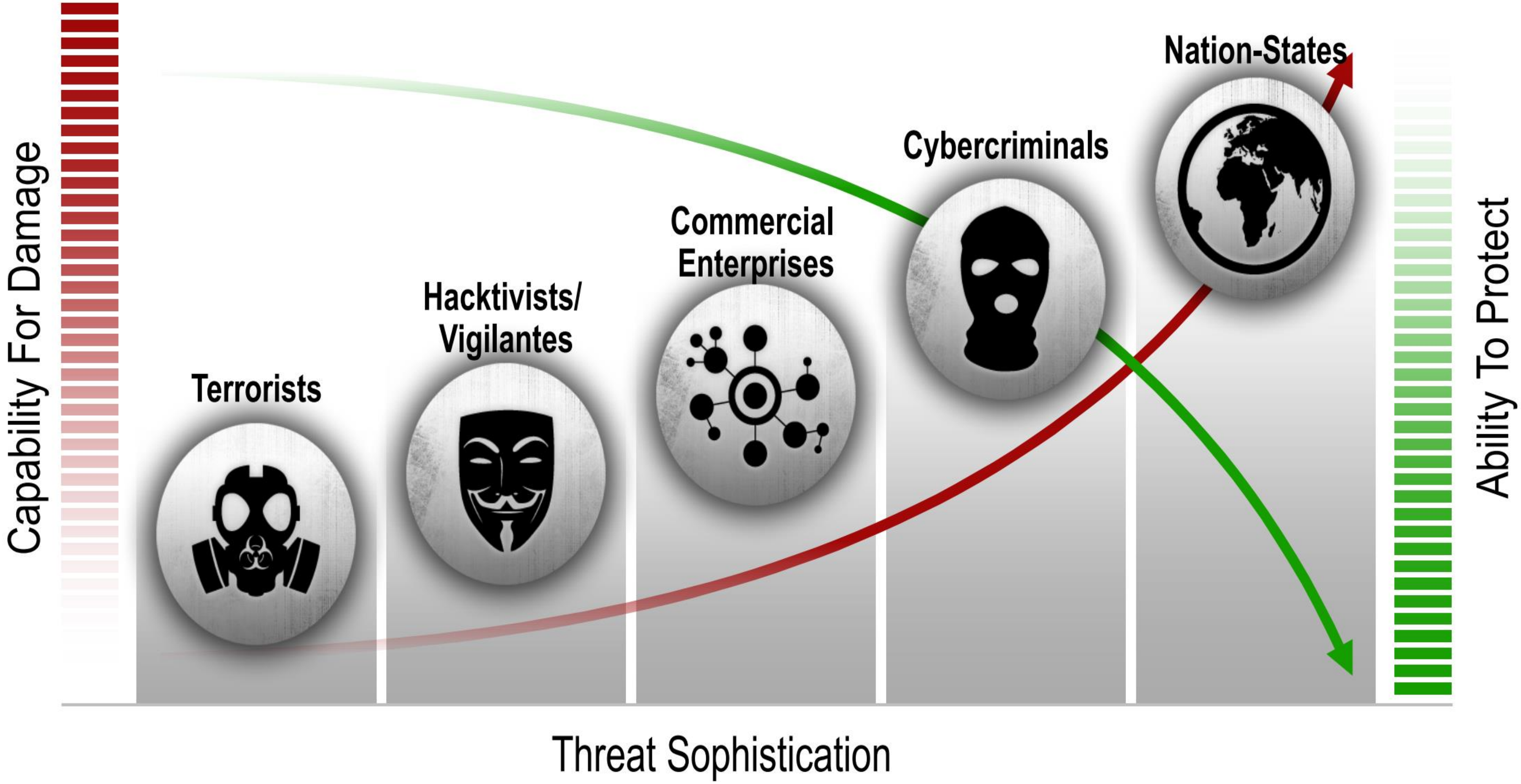
Nation states

Insiders

Cyber-terrorists / Hacktivists

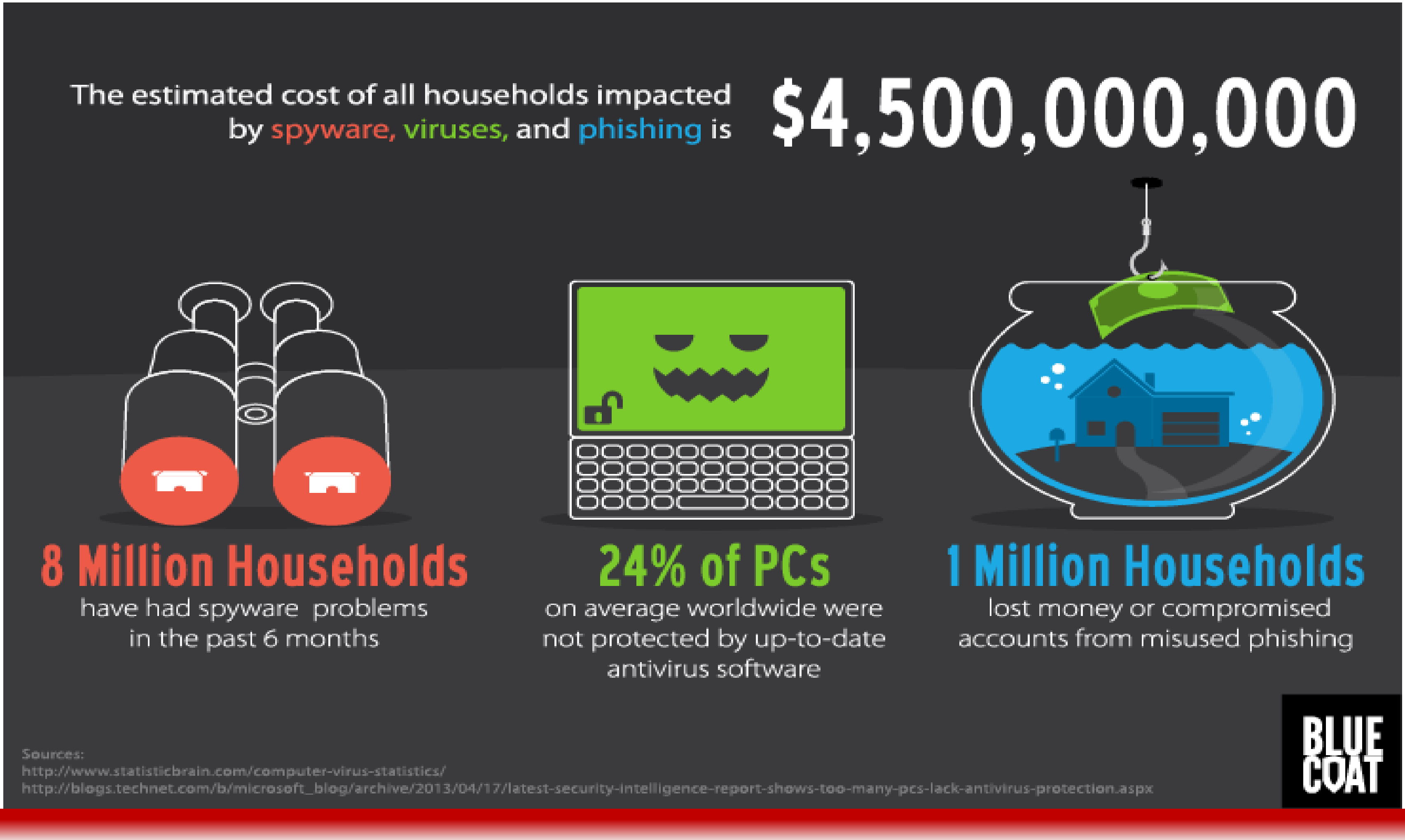
Others…

CYBER THREATS



SC CYBER

Cyber Threats



The estimated cost of all households impacted by spyware, viruses, and phishing is **$4,500,000,000**

8 Million Households have had spyware problems in the past 6 months

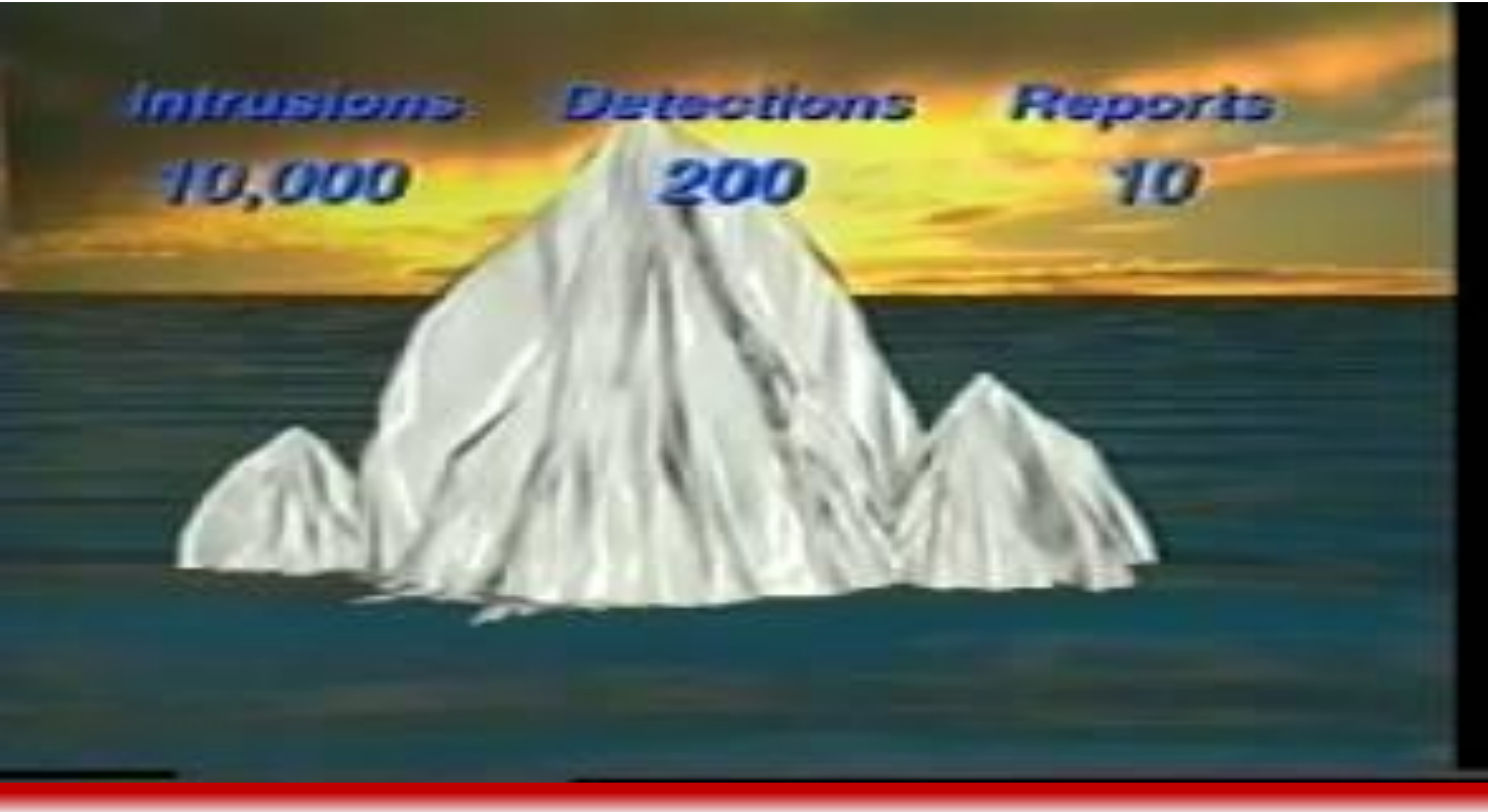
24% of PCs on average worldwide were not protected by up-to-date antivirus software

1 Million Households lost money or compromised accounts from misused phishing

Sources:
http://www.statisticbrain.com/computer-virus-statistics/
http://blogs.technet.com/b/microsoft_blog/archive/2013/04/17/latest-security-intelligence-report-shows-too-many-pcs-lack-antivirus-protection.aspx

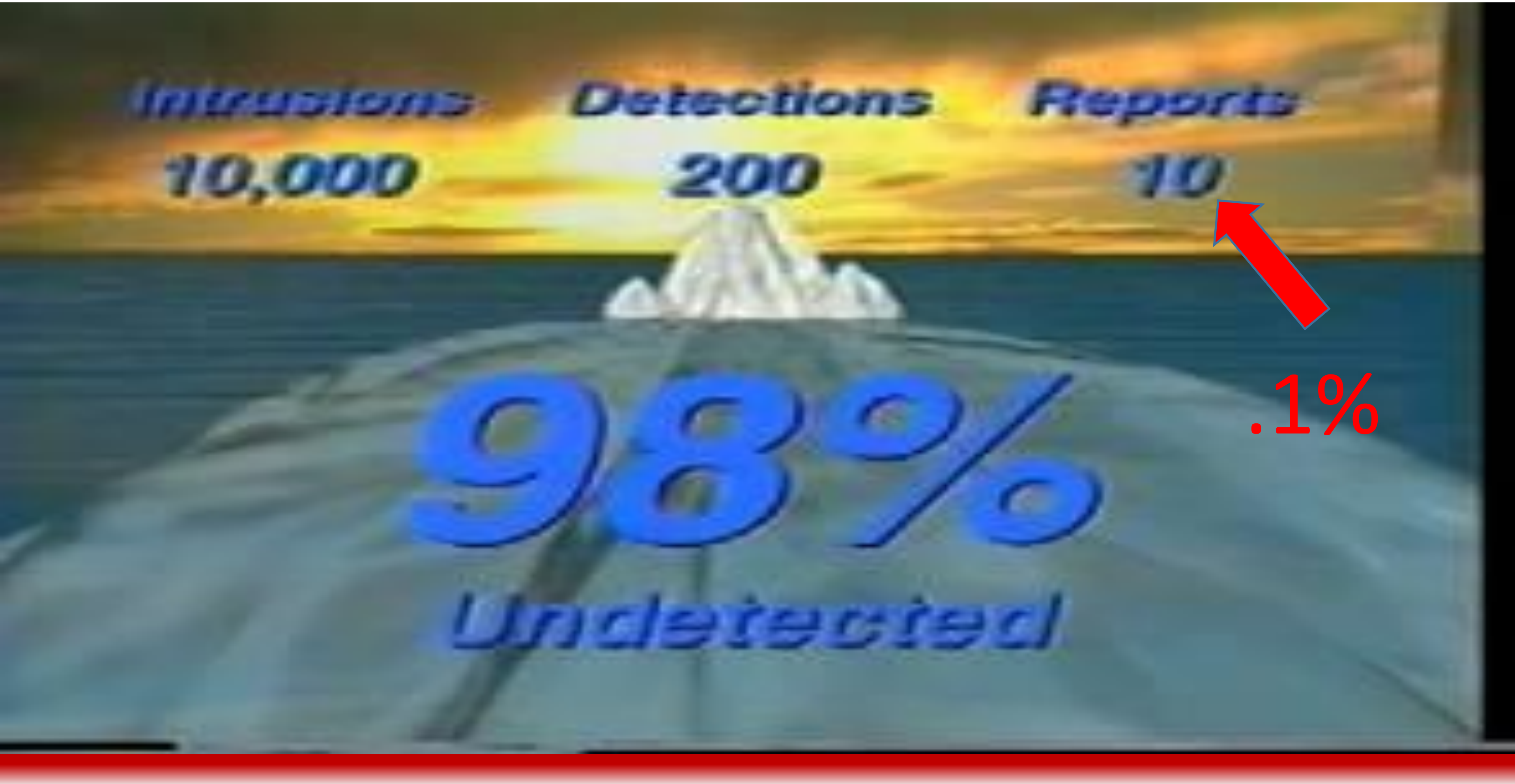
BLUE COAT

Its What You Don’t See….



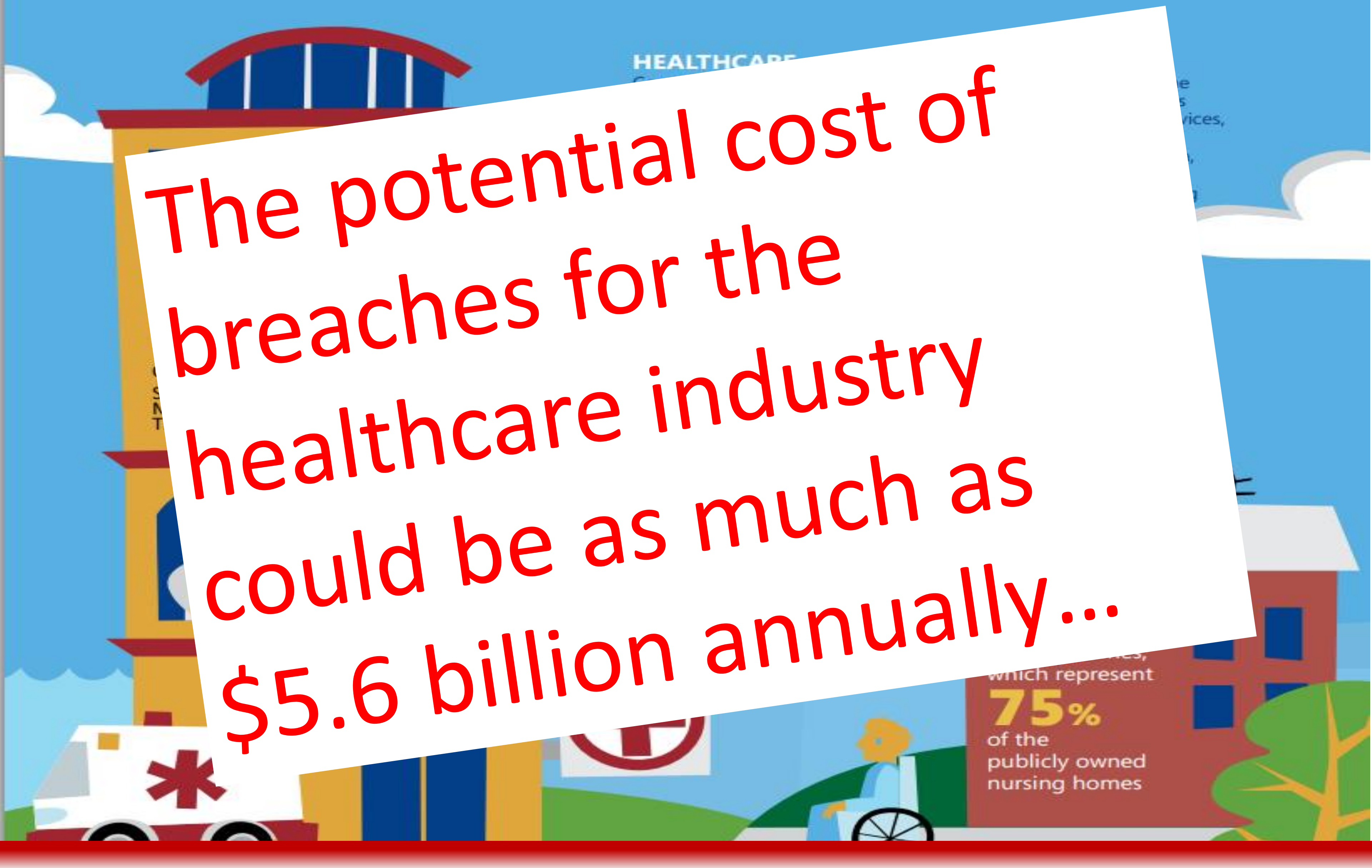
SC CYBER

…that is SCARY!!!



SC CYBER

U.S. companies reported $40 billion in losses from unauthorized use of computers by employees in 2014…

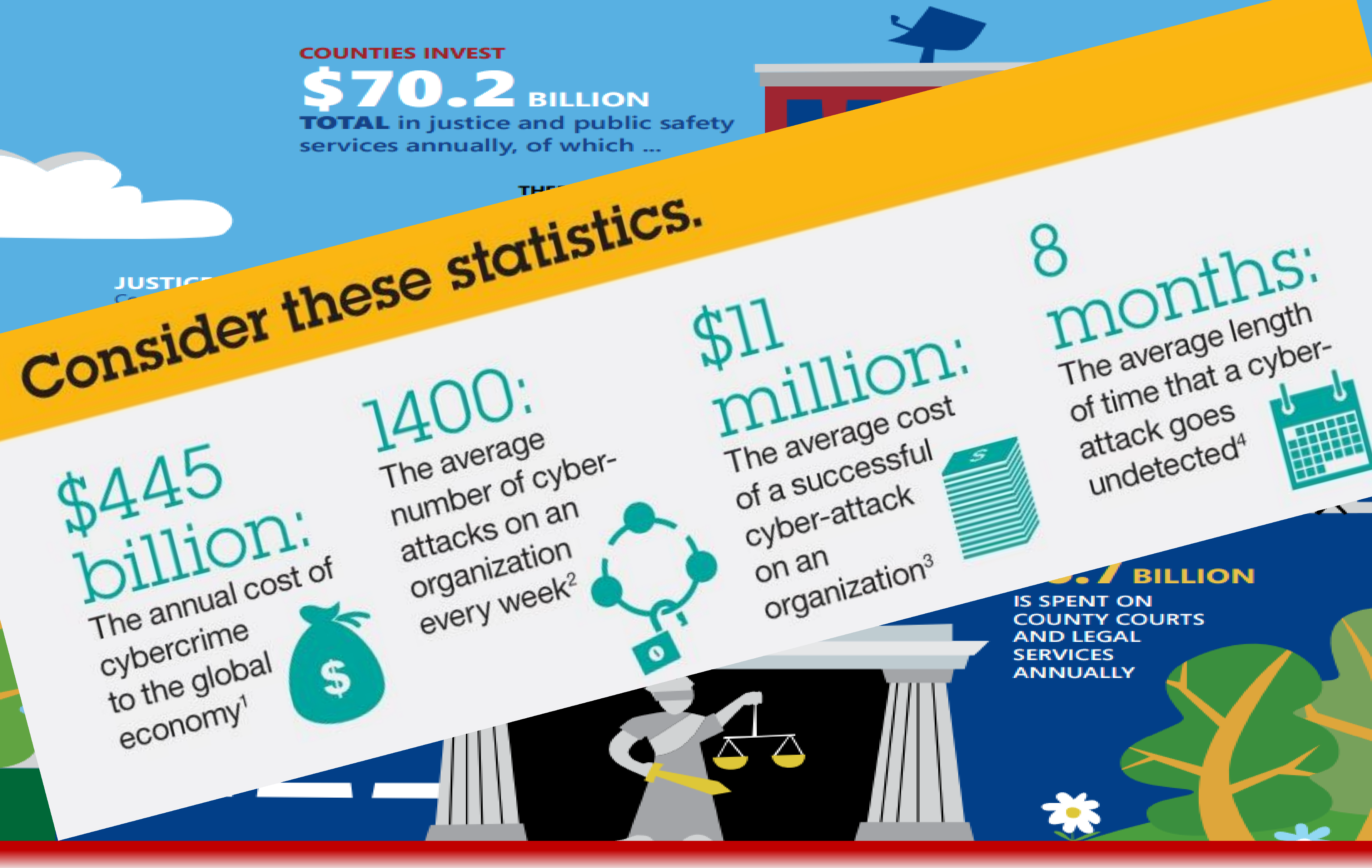


The potential cost of breaches for the healthcare industry could be as much as $5.6 billion annually…

There are over 7,200 industrial control systems directly linked to the internet...

TRANSPORTATION & INFRASTRUCTURE
Transportation and infrastructure are critical components that suppor
of living for all Americans. By providing efficient transpor
systems, counties are the driving force conn
the hospitals that treat and pro
up storm debris
ndard
vay
arn,
ning
on
TIES INVEST
2.3
ION
onstruction
lic facilities
annually
OWN AND MAINTAIN
45% of America's roads
COUNTIES INVEST
$106.3 BILLION
IN BUILDING INFRASTRUCTURE AND MAINTAINING AND OPERATING PUBLIC WORKS ANNUALLY
COUNTIES ARE INVOLVED in 27% of public transit systems
COUNTIES INVEST
$18.6 BILLION
in sewage and solid waste management annually

SC CYBER



COUNTIES INVEST

$70.2 BILLION

TOTAL in justice and public safety services annually, of which ...

.7 BILLION

IS SPENT ON COUNTY COURTS AND LEGAL SERVICES ANNUALLY

Consider these statistics.

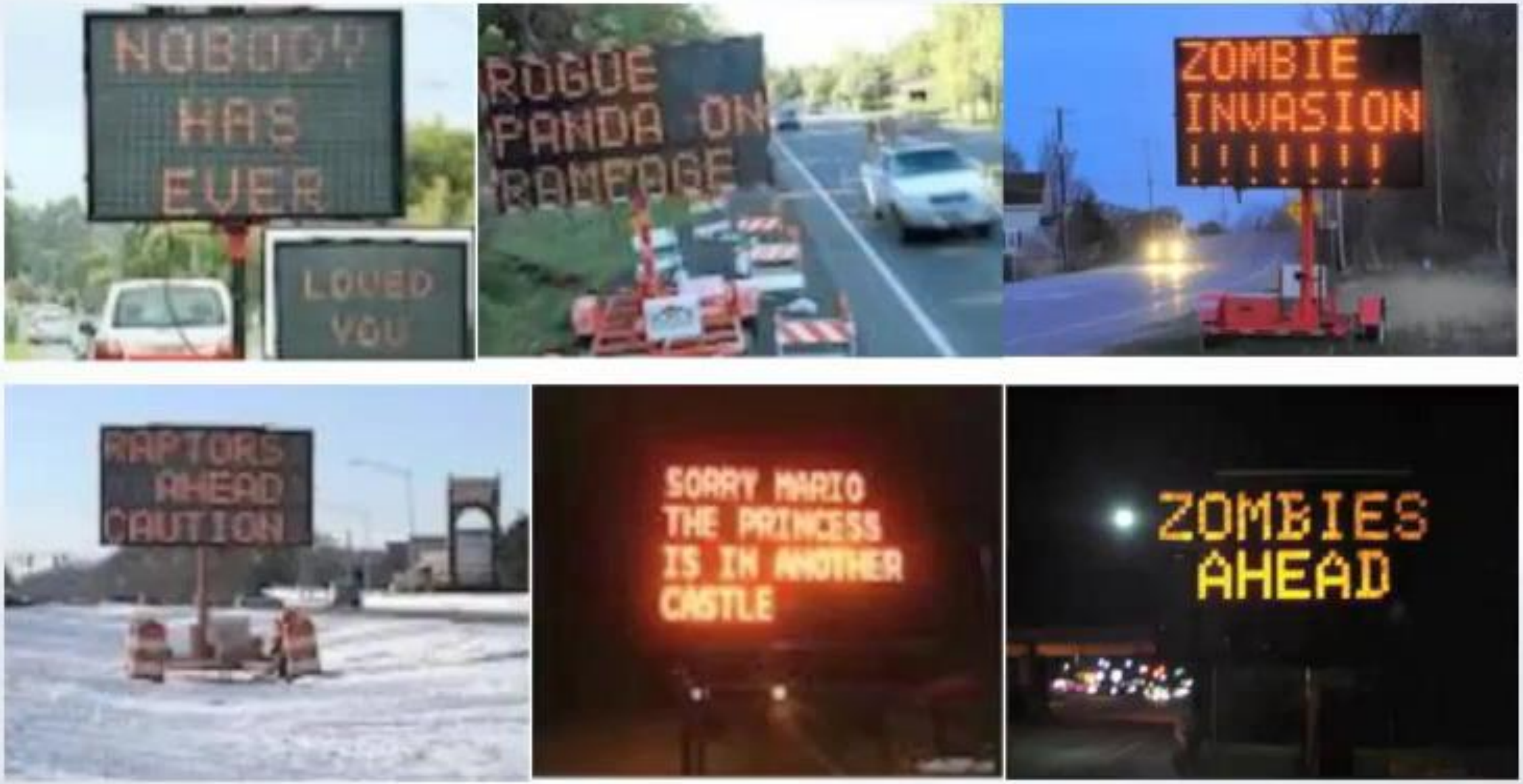
$445 billion: The annual cost of cybercrime to the global economy[1]

1400: The average number of cyber-attacks on an organization every week[2]

$11 million: The average cost of a successful cyber-attack on an organization[3]

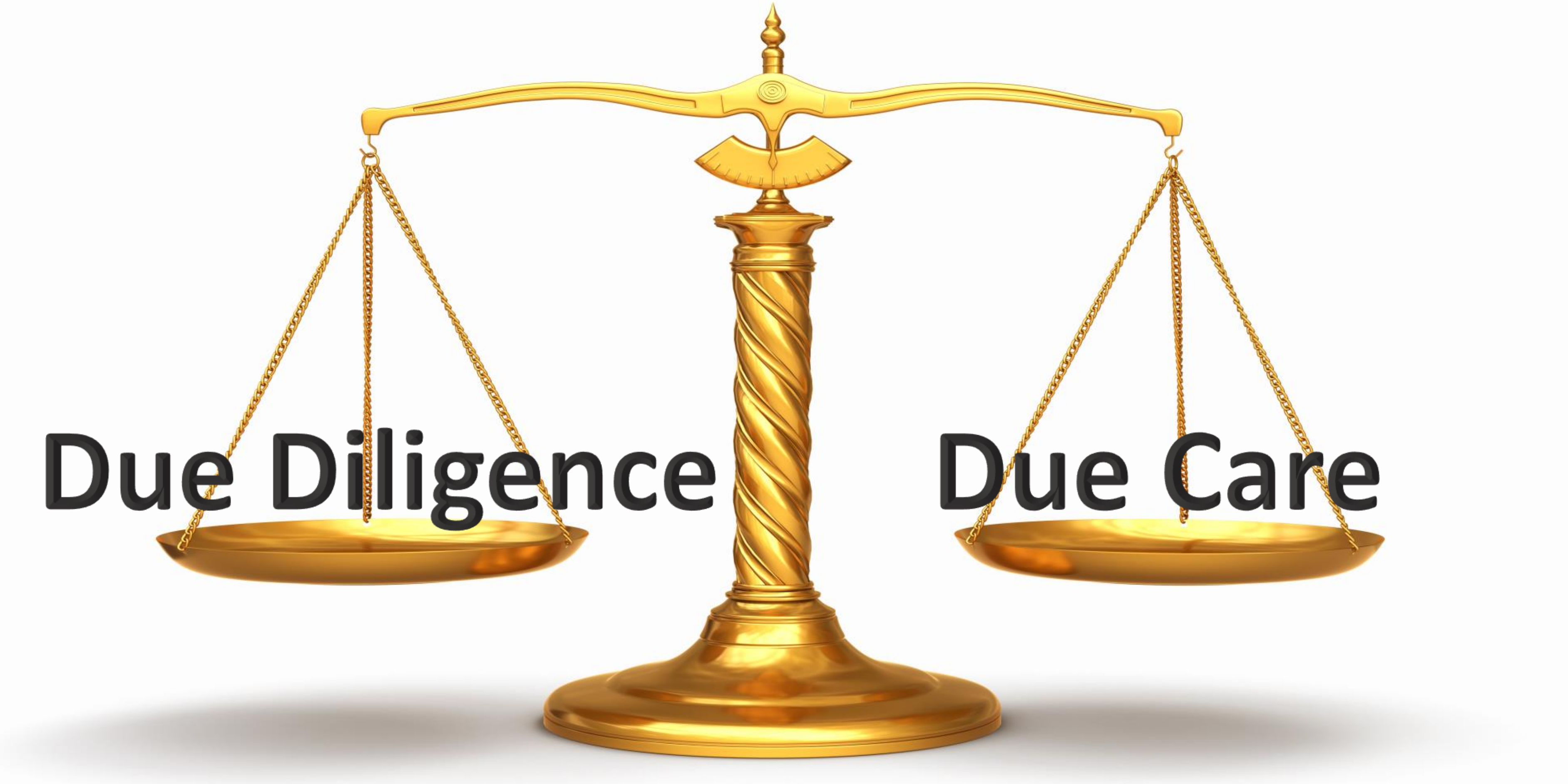
8 months: The average length of time that a cyber-attack goes undetected[4]

Frequent Hacks Into Highway Dynamic Message Signs



Computer incident response was once the sole responsibility of the IT department, but as it has become clear that the consequences of a computer incident can threaten an enterprise’s very existence, directors are now being held more accountable.

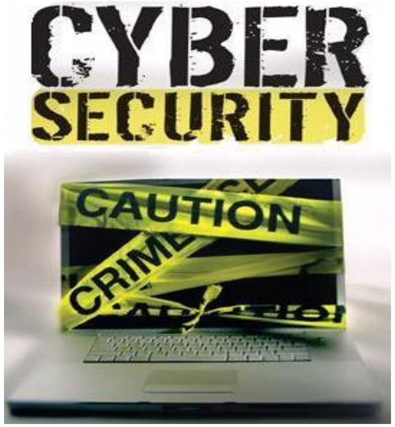
Directors have to be aware that a serious computer incident could result in a number of negative consequences for their enterprise, such as reputational damage or regulatory fines

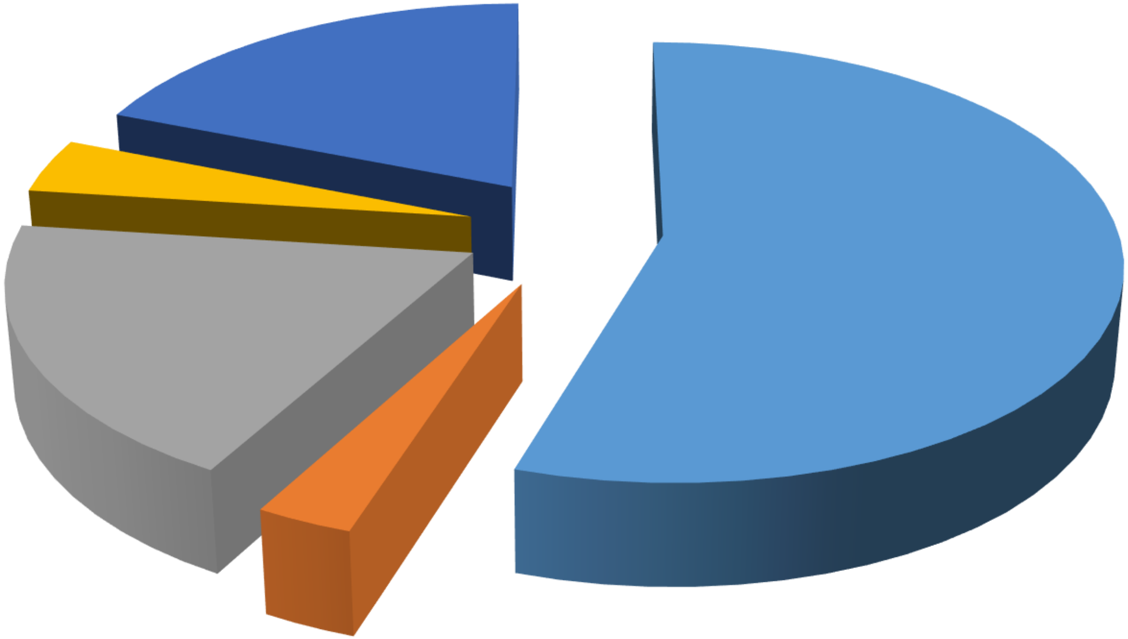


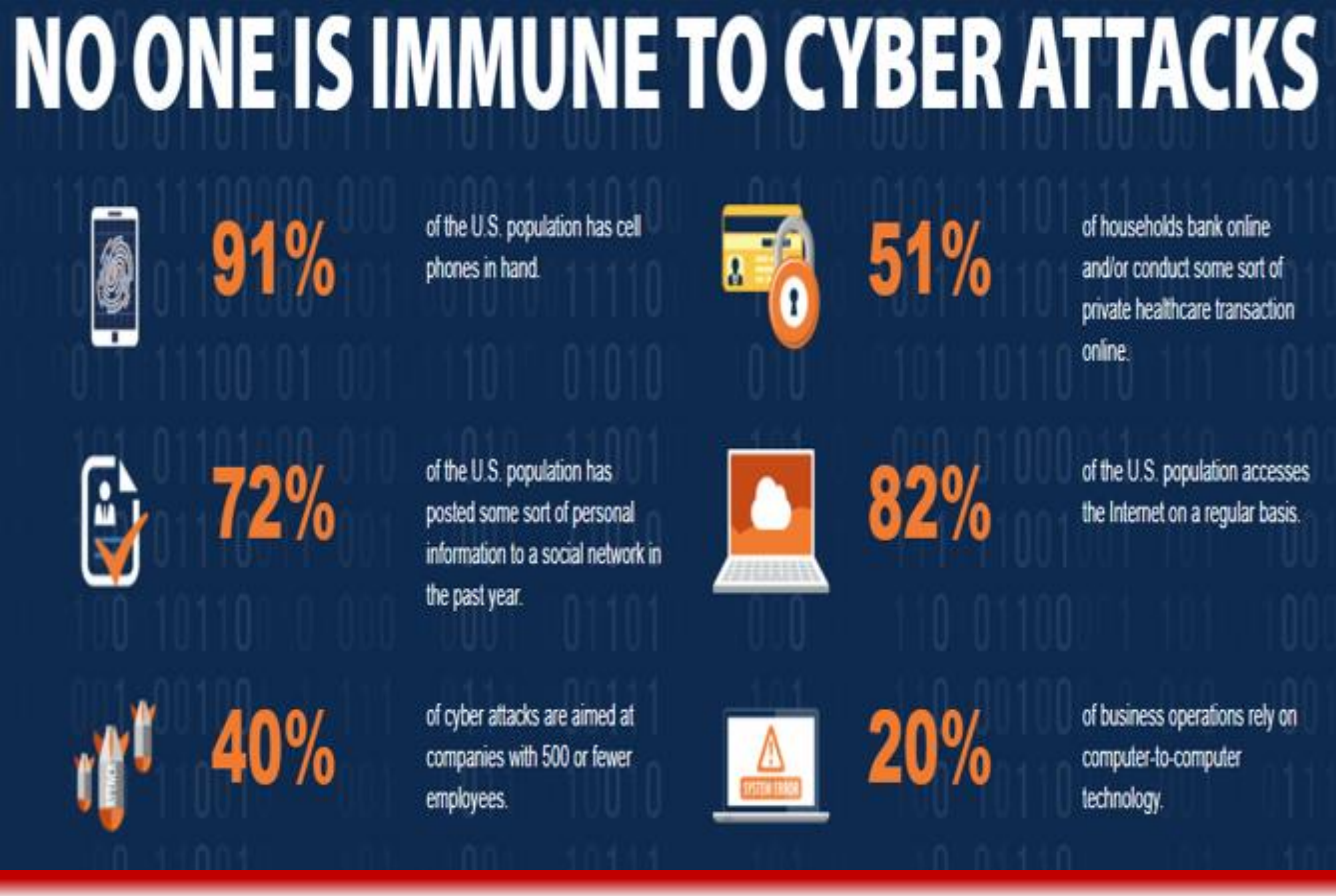
Due Diligence

Due Care

Computer Crime







NO ONE IS IMMUNE TO CYBER ATTACKS

91% of the U.S. population has cell phones in hand.

51% of households bank online and/or conduct some sort of private healthcare transaction online.

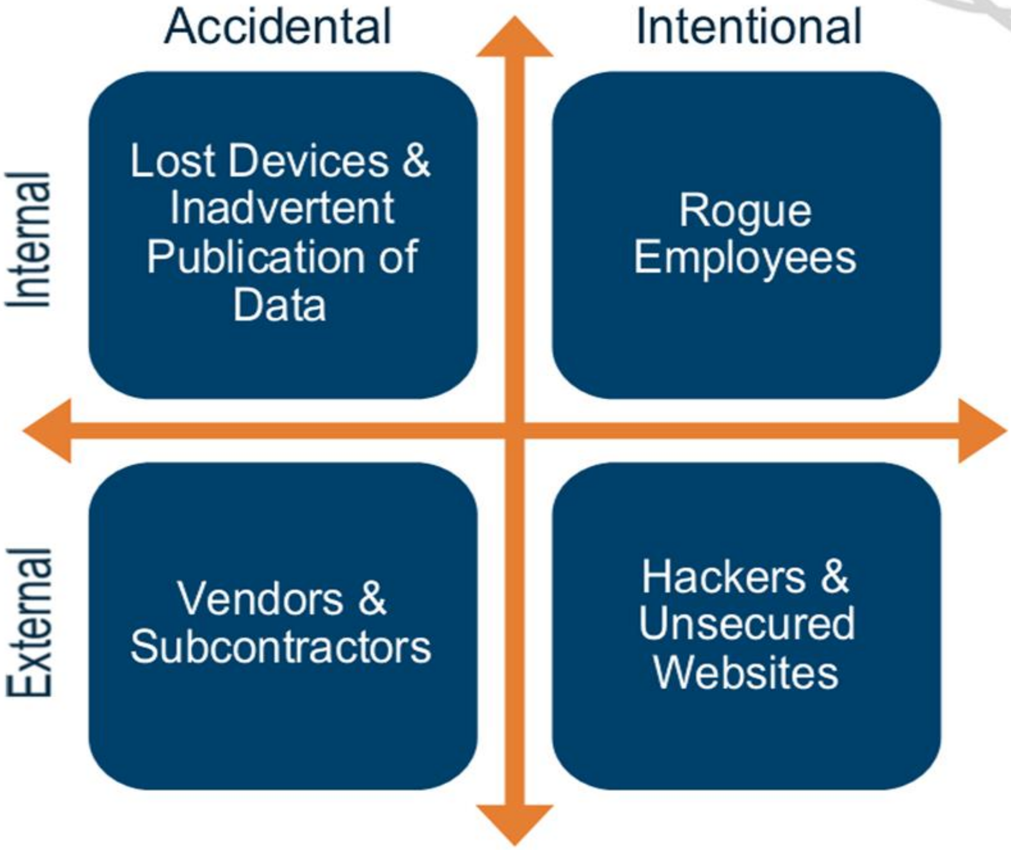
72% of the U.S. population has posted some sort of personal information to a social network in the past year.

82% of the U.S. population accesses the Internet on a regular basis.

40% of cyber attacks are aimed at companies with 500 or fewer employees.

20% of business operations rely on computer-to-computer technology.

How Do Incidents Occur?



	Accidental	Intentional
Internal	Lost Devices & Inadvertent Publication of Data	Rogue Employees
External	Vendors & Subcontractors	Hackers & Unsecured Websites

Small businesses experience most of the data breach incidents because they:

- Are less aware of their exposures
- Have fewer resources to provide appropriate data protection and/or security awareness training for employees
- Are less likely to have strong cyber risk management controls in place
- Typically do not have a dedicated risk management professional
- Serve as a training ground for cyber thieves who are honing their skills to prepare for bigger attacks
- Are less likely to discover data breach

TIME IS **MONEY**

Cyber attacks can get costly if not resolved quickly. Results show a positive relationship between the time to contain an attack and organizational cost.[1]

RSA Warns SecurID Customers of Breach

DDOS Attacks by Iran on Top U.S. Banks

OPM Breach -Foreign Spies In Our Government Data

NYT, WSJ, and Washington Post Claim to be Hacked by Chinese

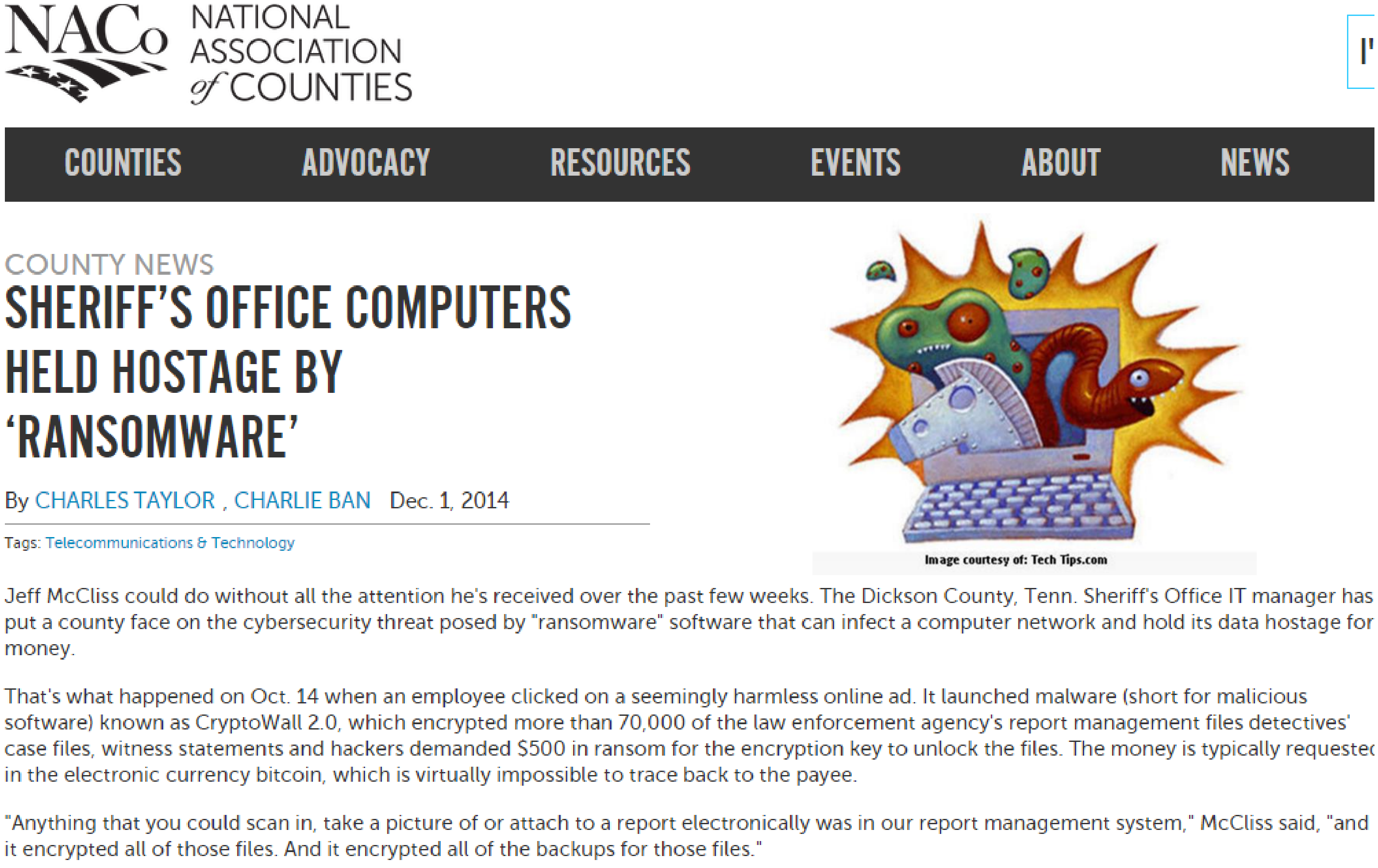
DNC hacked by Russians, posted on WikiLeaks

Criminal Ring Steals Millions of Identities from Heath Insurance Company

Sony, JP Morgan and Target all taken down by hackers

SC CYBER

Could this happen to you?



COUNTY NEWS

SHERIFF'S OFFICE COMPUTERS HELD HOSTAGE BY 'RANSOMWARE'

By CHARLES TAYLOR , CHARLIE BAN Dec. 1, 2014

Tags: Telecommunications & Technology

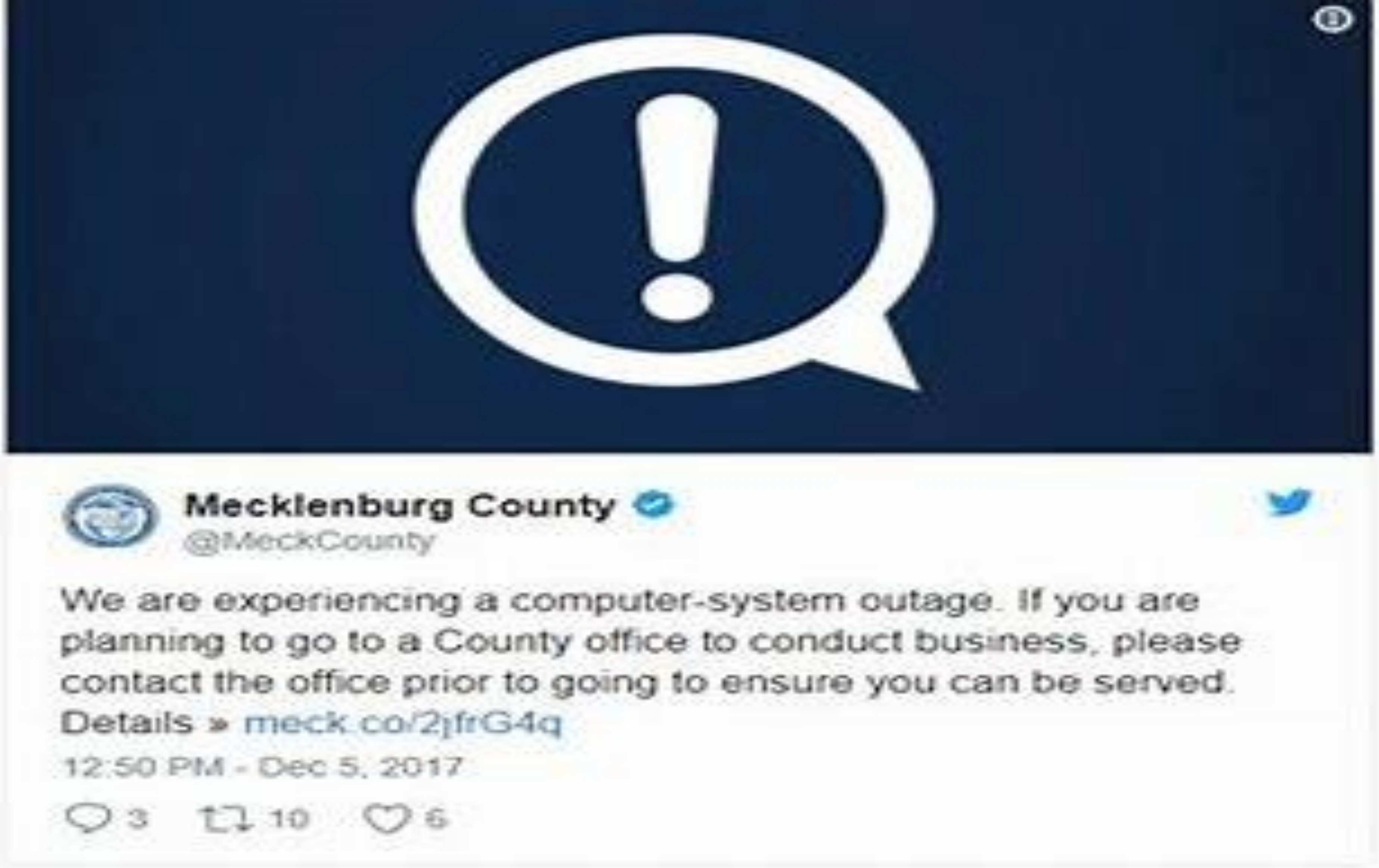
Image courtesy of: Tech Tips.com

Jeff McCliss could do without all the attention he's received over the past few weeks. The Dickson County, Tenn. Sheriff's Office IT manager has put a county face on the cybersecurity threat posed by "ransomware" software that can infect a computer network and hold its data hostage for money.

That's what happened on Oct. 14 when an employee clicked on a seemingly harmless online ad. It launched malware (short for malicious software) known as CryptoWall 2.0, which encrypted more than 70,000 of the law enforcement agency's report management files detectives' case files, witness statements and hackers demanded $500 in ransom for the encryption key to unlock the files. The money is typically requestec in the electronic currency bitcoin, which is virtually impossible to trace back to the payee.

"Anything that you could scan in, take a picture of or attach to a report electronically was in our report management system," McCliss said, "and it encrypted all of those files. And it encrypted all of the backups for those files."

MECKLENBURG COUNTY
NORTH CAROLINA
MAY 20, 1775



Mecklenburg County
@MeckCounty

We are experiencing a computer-system outage. If you are planning to go to a County office to conduct business, please contact the office prior to going to ensure you can be served. Details » meck.co/2jfrG4q

12:50 PM - Dec 5, 2017

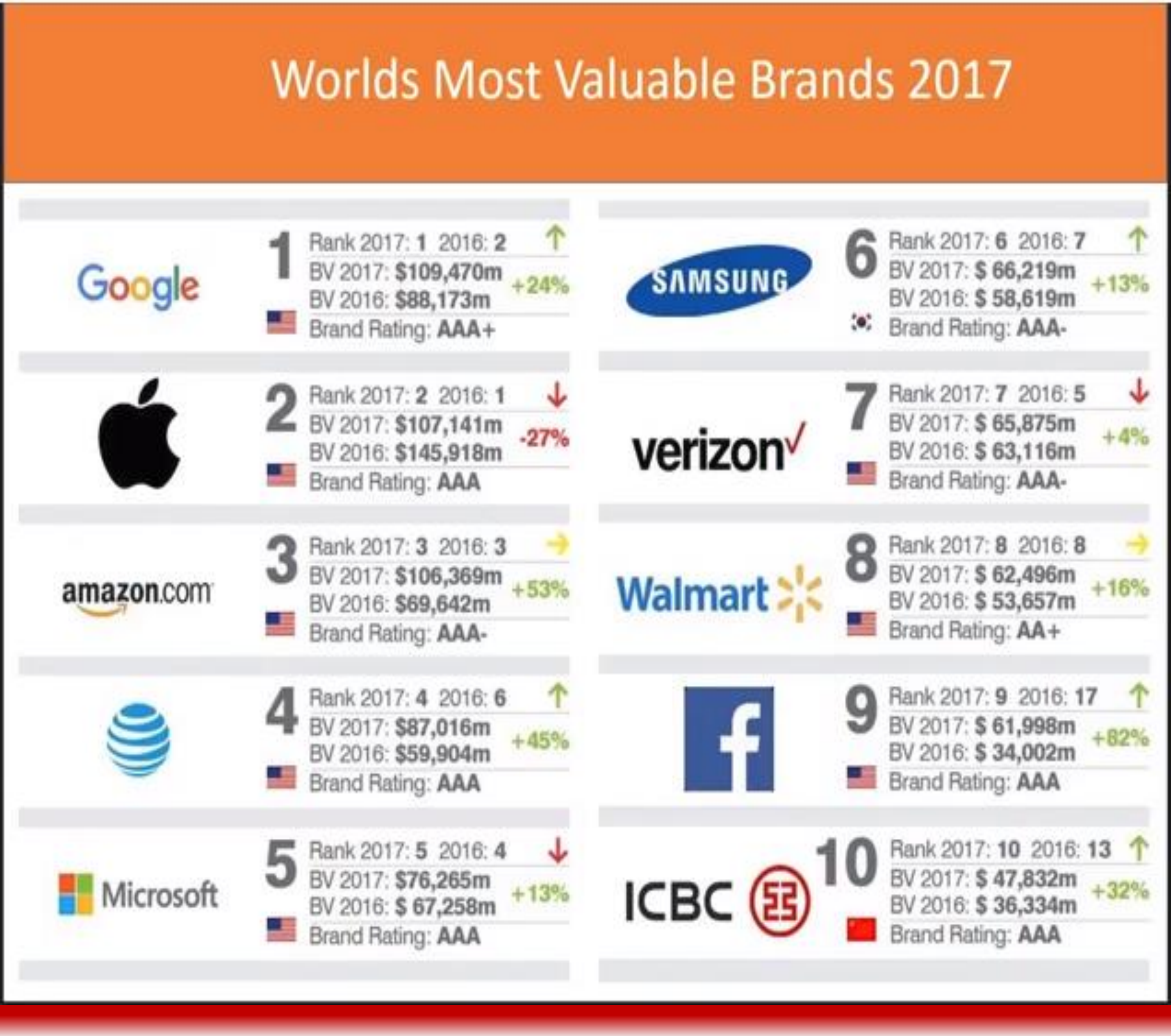
I shall infect network servers with something called "Ransomware" and hold an organization's data hostage for...

40 BITCOINS

All have had Security Incidents

Some have had well documented data breaches

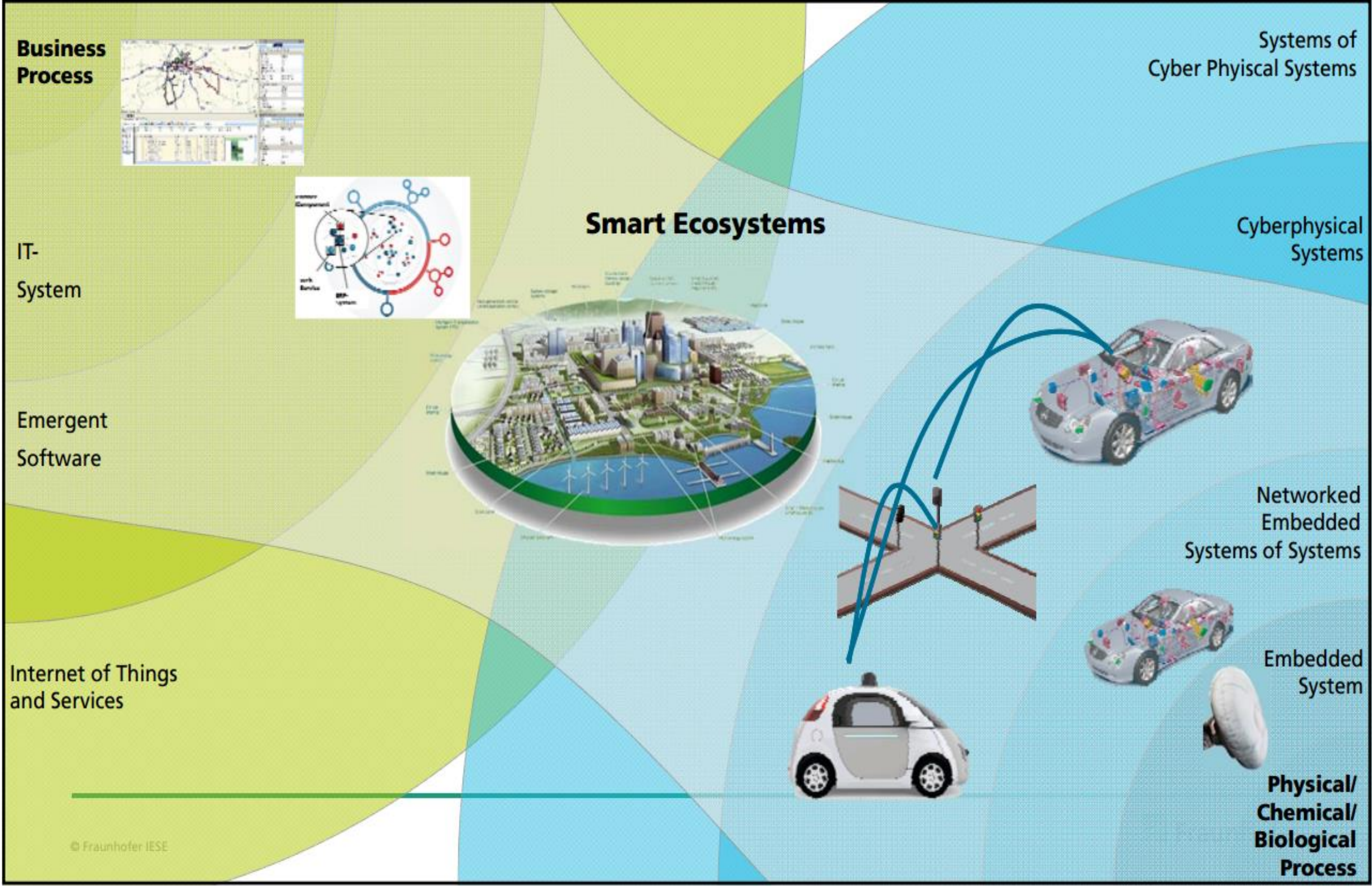
Yet, they minimized Brand Erosion



Worlds Most Valuable Brands 2017

Google	1	Rank 2017: 1 2016: 2	↑	BV 2017: $109,470m	BV 2016: $88,173m	+24%	Brand Rating: AAA+
	2	Rank 2017: 2 2016: 1	↓	BV 2017: $107,141m	BV 2016: $145,918m	-27%	Brand Rating: AAA
amazon.com	3	Rank 2017: 3 2016: 3	→	BV 2017: $106,369m	BV 2016: $69,642m	+53%	Brand Rating: AAA-
	4	Rank 2017: 4 2016: 6	↑	BV 2017: $87,016m	BV 2016: $59,904m	+45%	Brand Rating: AAA
Microsoft	5	Rank 2017: 5 2016: 4	↓	BV 2017: $76,265m	BV 2016: $ 67,258m	+13%	Brand Rating: AAA
SAMSUNG	6	Rank 2017: 6 2016: 7	↑	BV 2017: $ 66,219m	BV 2016: $ 58,619m	+13%	Brand Rating: AAA-
verizon	7	Rank 2017: 7 2016: 5	↓	BV 2017: $ 65,875m	BV 2016: $ 63,116m	+4%	Brand Rating: AAA-
Walmart	8	Rank 2017: 8 2016: 8	→	BV 2017: $ 62,496m	BV 2016: $ 53,657m	+16%	Brand Rating: AA+
f	9	Rank 2017: 9 2016: 17	↑	BV 2017: $ 61,998m	BV 2016: $ 34,002m	+82%	Brand Rating: AAA
ICBC	10	Rank 2017: 10 2016: 13	↑	BV 2017: $ 47,832m	BV 2016: $ 36,334m	+32%	Brand Rating: AAA

The Internet of Things!!



Business Process

IT-System

Emergent Software

Internet of Things and Services

Smart Ecosystems

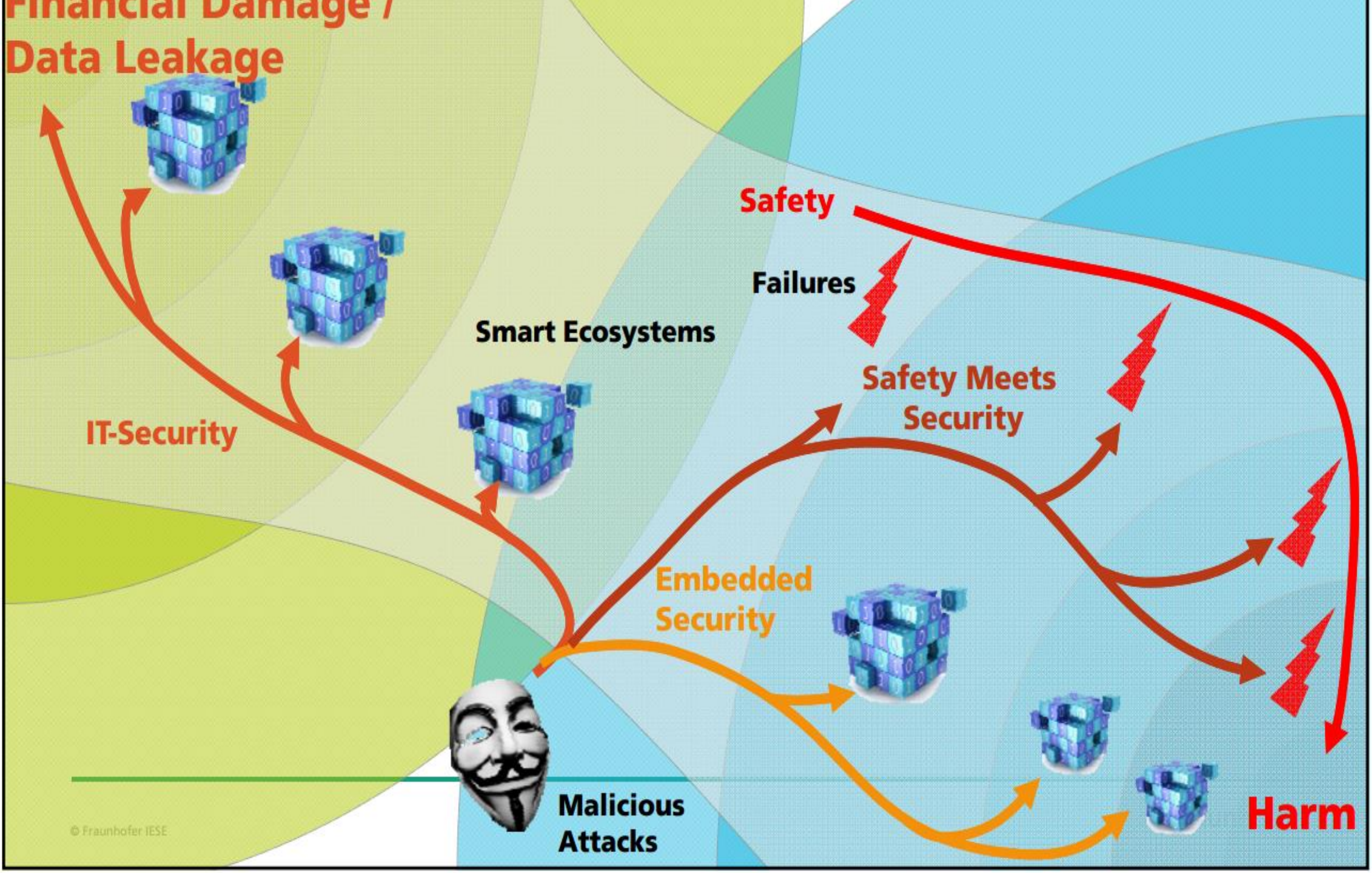
Systems of Cyber Phyiscal Systems

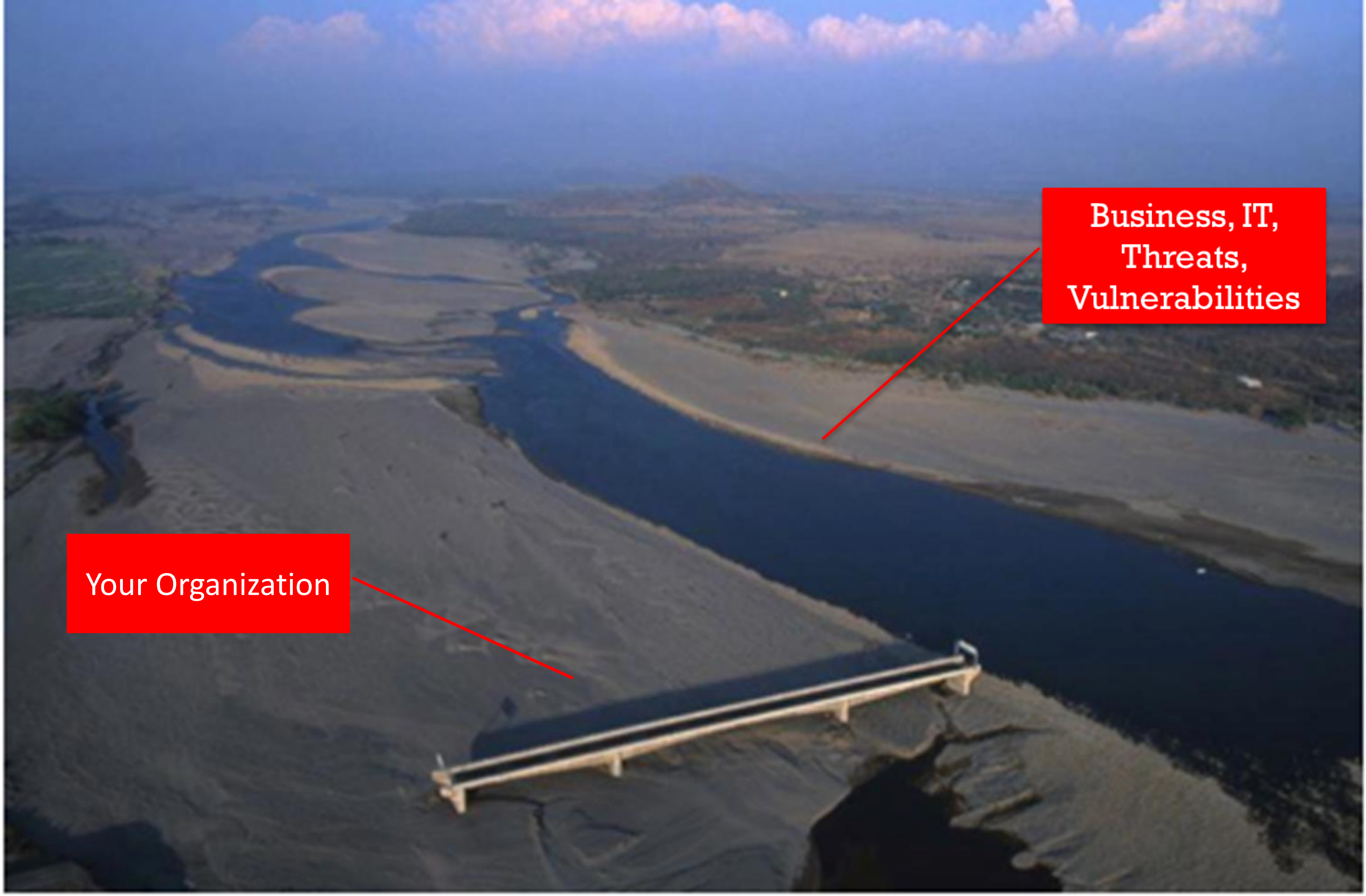
Cyberphysical Systems

Networked Embedded Systems of Systems

Embedded System

Physical/ Chemical/ Biological Process


Financial Damage /
Data Leakage
Safety
Failures
Smart Ecosystems
Safety Meets
Security
IT-Security
Embedded
Security
Malicious
Attacks
Harm
© Fraunhofer IESE


Business, IT,
Threats,
Vulnerabilities
Your Organization

FEAR

UNCERTAINTY

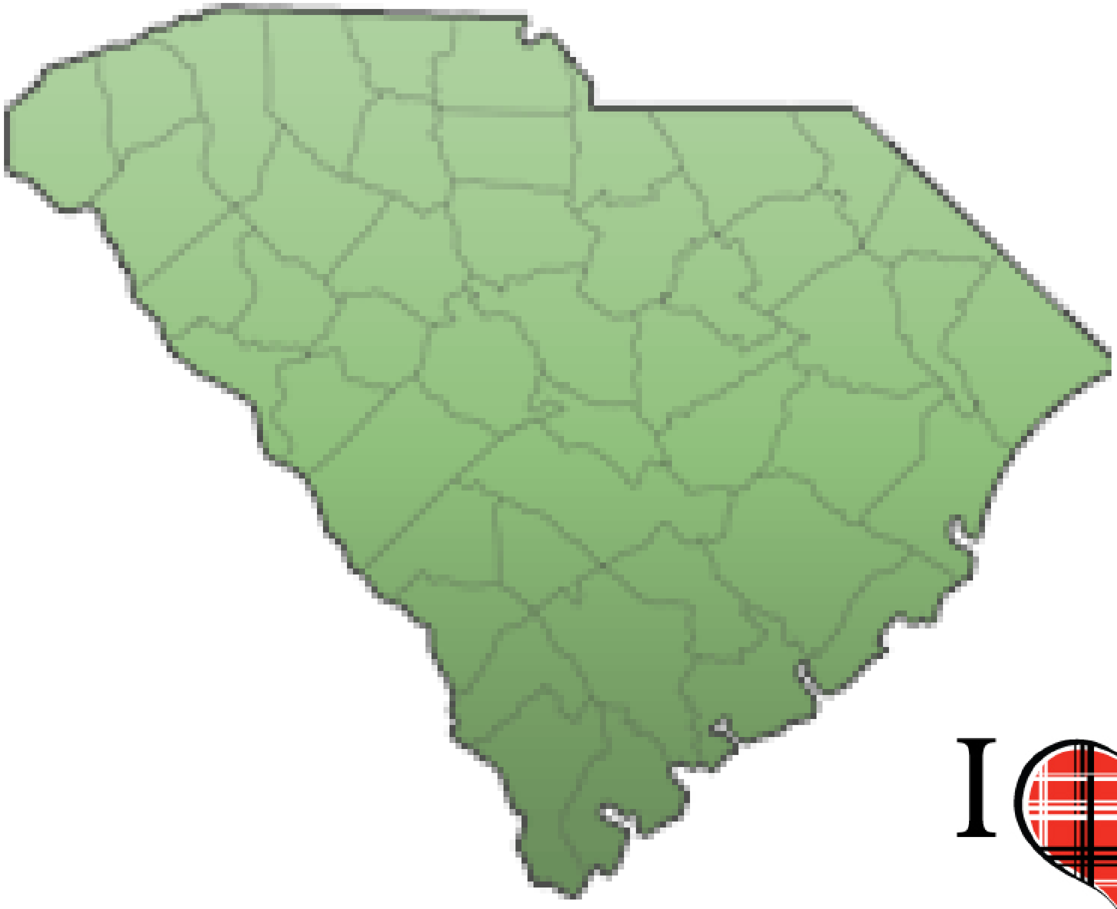
DOUBT

MANAGING YOUR RISK(S)

MANAGING YOUR RISKS

- Identify what information your county stores and uses
- Determine the value of your information
- Develop an inventory
- Understand your threats and vulnerabilities

Identify what information your county stores and uses



SCARE

South Carolina Association of Registration & Elections

South Carolina Clerks to Council Association

South Carolina Auditors, Treasurers and Tax Collectors SCATT Organized - 1947 -

South Carolina Coroner's Association

JUSTICE

South Carolina Emergency Management Association

I ❤ my public library

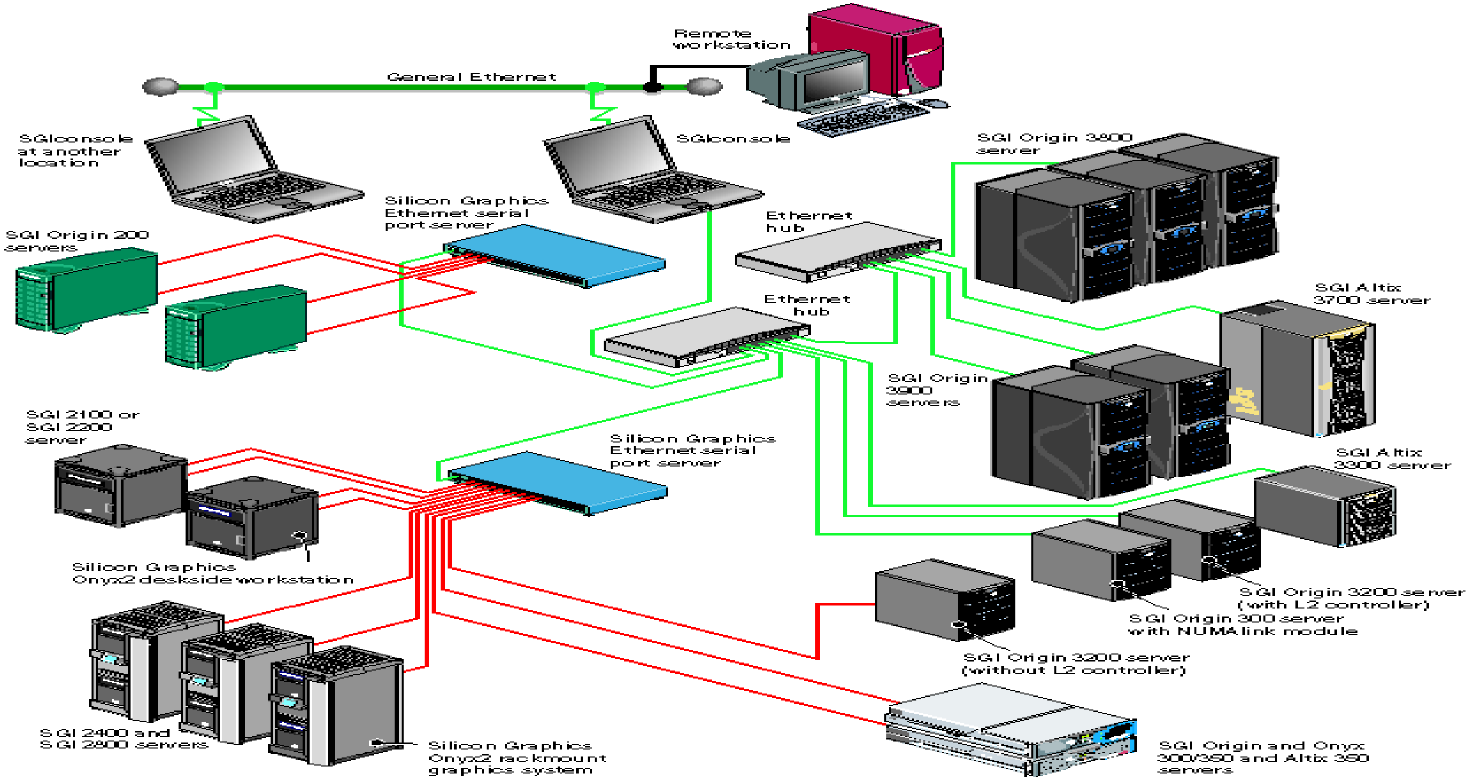
SC CYBER

Determine the value of your information

SC CYBER

MANAGING YOUR RISKS

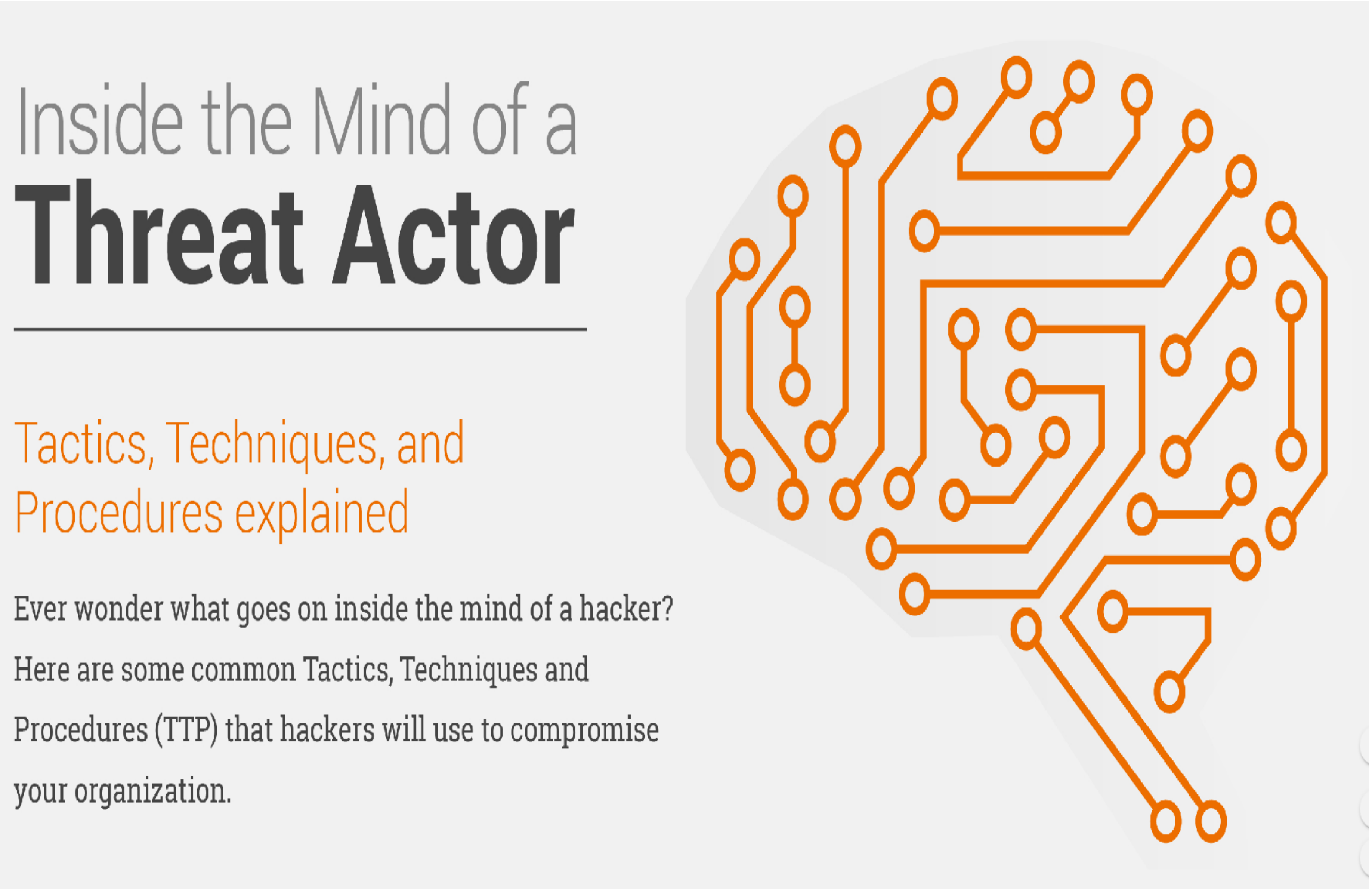
- Develop an inventory



Remote workstation
General Ethernet
SGIconsole at another location
SGIconsole
SGI Origin 3800 server
Silicon Graphics Ethernet serial port server
Ethernet hub
SGI Origin 200 servers
Ethernet hub
SGI Altix 3700 server
SGI Origin 3900 servers
SGI 2100 or SGI 2200 server
Silicon Graphics Ethernet serial port server
SGI Altix 3300 server
Silicon Graphics Onyx2 deskside workstation
SGI Origin 3200 server (with L2 controller)
SGI Origin 300 server with NUMAlink module
SGI Origin 3200 server (without L2 controller)
SGI 2400 and SGI 2800 servers
Silicon Graphics Onyx2 rackmount graphics system
SGI Origin and Onyx 300/350 and Altix 350 servers

What are they really after?

- Your Intellectual Property
- Your assets
- Your customer data
- Your personal data
- Your paycheck
- Your friends
- Your family



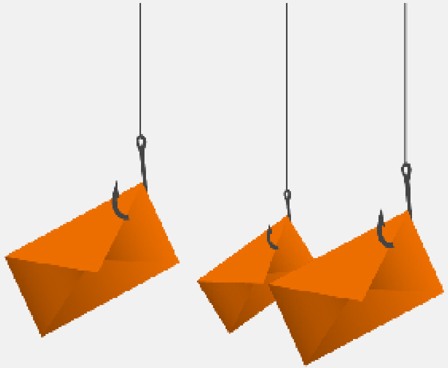
Inside the Mind of a **Threat Actor**

Tactics, Techniques, and Procedures explained

Ever wonder what goes on inside the mind of a hacker? Here are some common Tactics, Techniques and Procedures (TTP) that hackers will use to compromise your organization.

Phishing

It sounds like old news and yet it's so effective that hackers will keep using this tactic.



Untargeted Attacks

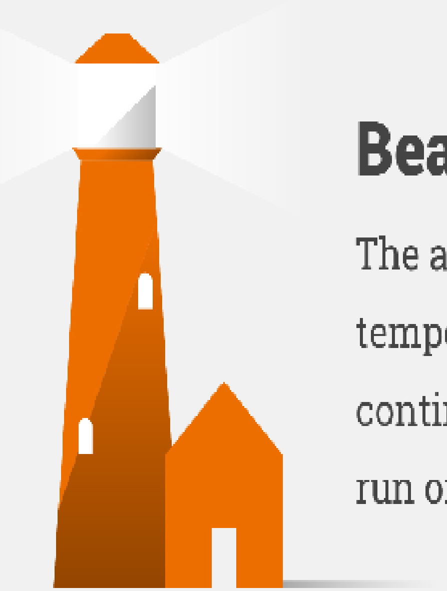
Hackers can send phishing emails all over the internet in hopes of a bite. It can arrive as an email about your shipment delivery or from your "IT Department" requesting a password change.

Targeted Attacks

Sometimes hackers want something specifically that only YOU have access to... so you'll be targeted with a convincing email: with legitimate company headers, email signatures, etc.

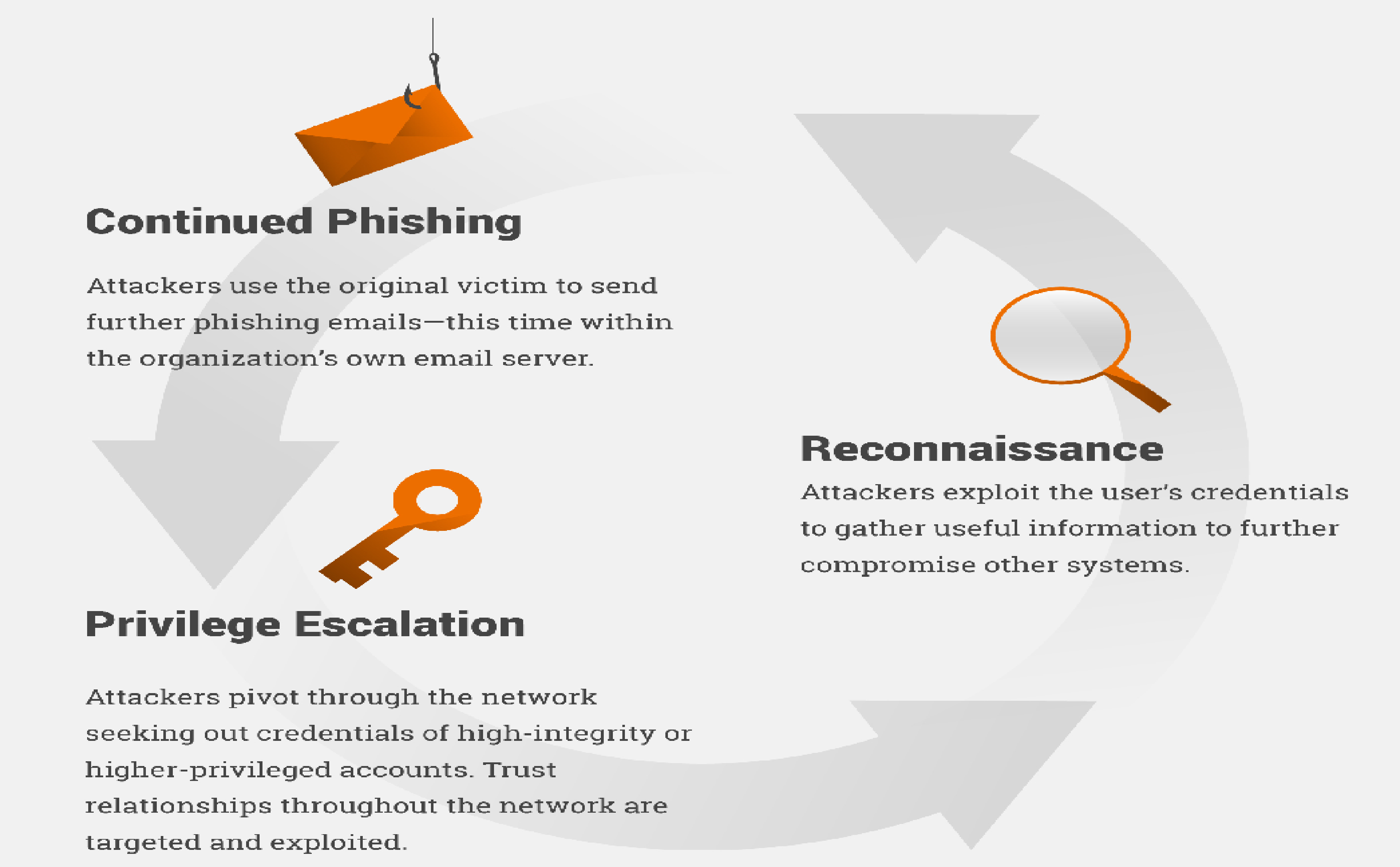
Digging in

When the hacker has an "in," they can employ a slew of other techniques and procedures to infiltrate deeper into your systems.



Beaconing

The attacker can install a way to get back into a compromised computer even if its temporarily disconnected from the internet, such as a beacon. The beacon will then continue to "call out" to the internet and check for commands (from the attacker) to run on the victim machine.



Continued Phishing

Attackers use the original victim to send further phishing emails—this time within the organization's own email server.

Reconnaissance

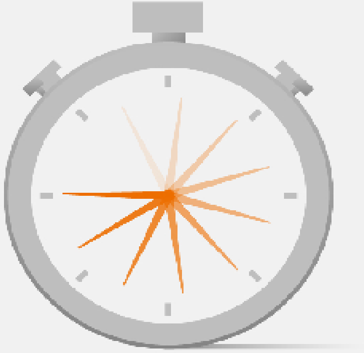
Attackers exploit the user's credentials to gather useful information to further compromise other systems.

Privilege Escalation

Attackers pivot through the network seeking out credentials of high-integrity or higher-privileged accounts. Trust relationships throughout the network are targeted and exploited.

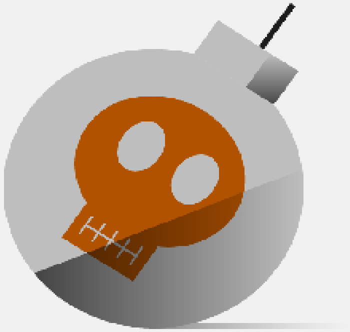
Exploitation

Once you've been compromised, hackers can find ways to continue the damage.



Long-term persistence

Hackers can perform beaconing stretched over long periods. Since the activity occurs so infrequently it becomes harder to detect. This allows hackers to harvest data over weeks, months, and sometimes years.



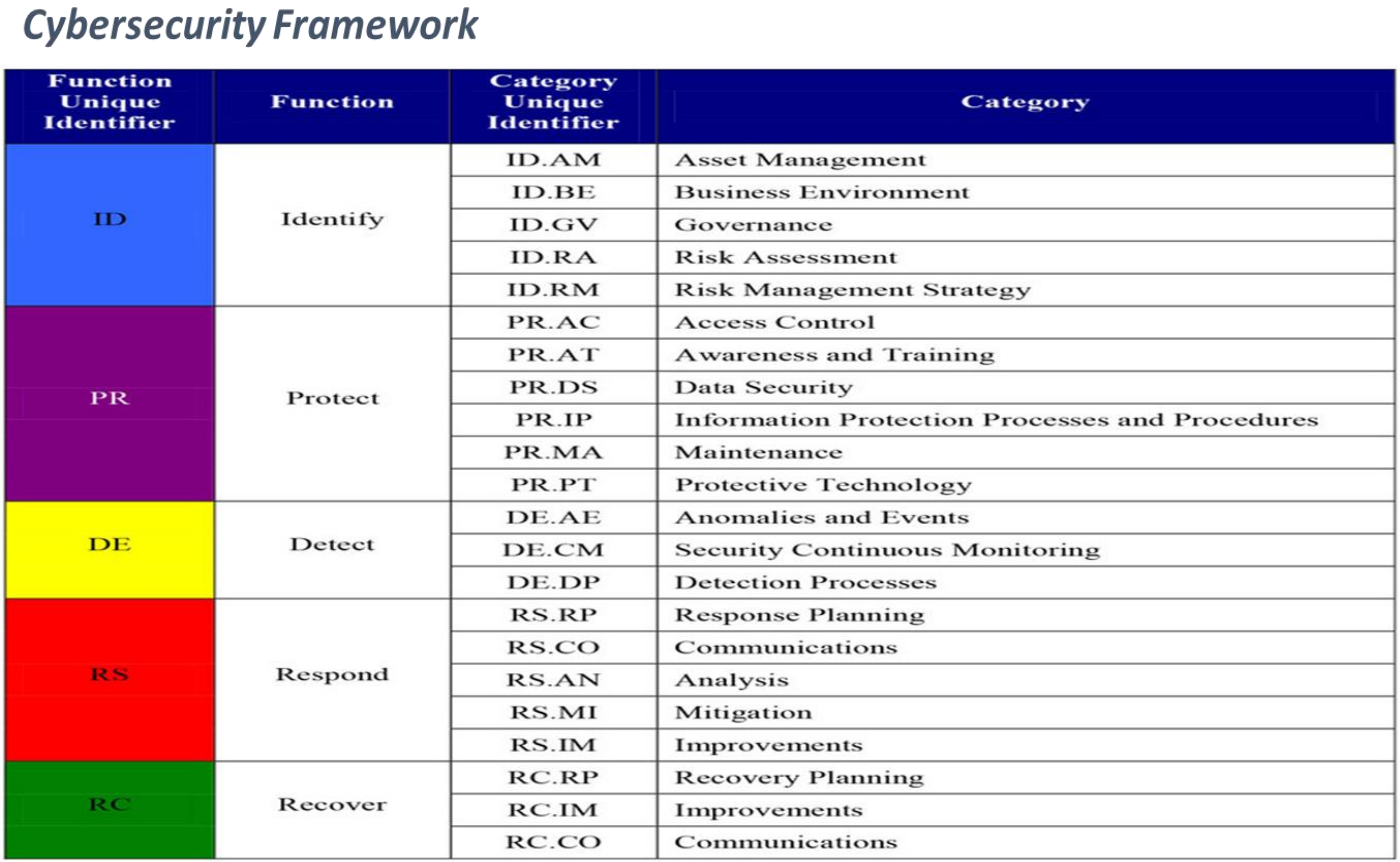
Destruction or Denial of Service

In the case of a total compromise, hackers can alter and/or destroy access. The most effective attacks begin weeks or months before leading to more overt and destructive activities.

Are you as well protected?

SC CYBER

NIST Cyber Security Framework (CSF)



Cybersecurity Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

IDENTIFY

- Identify and control who has access to your information

- Conduct Background Checks

- Require individual user accounts for each employee

- Create policies and procedures for information security

IDENTIFY

- Identify and control who has access to your information

"YOU REMEMBER DAVE. YOU STOLE HIS IDENTITY LAST YEAR."

IDENTIFY

- Conduct Background Checks

BACKGROUND CHECK
☑ Social Security verified
☑ Drug test
□ Driving record
□ Credit report
□ Criminal record
ILLUSTRATION: GWEN SUNG/CNNMONEY

IDENTIFY

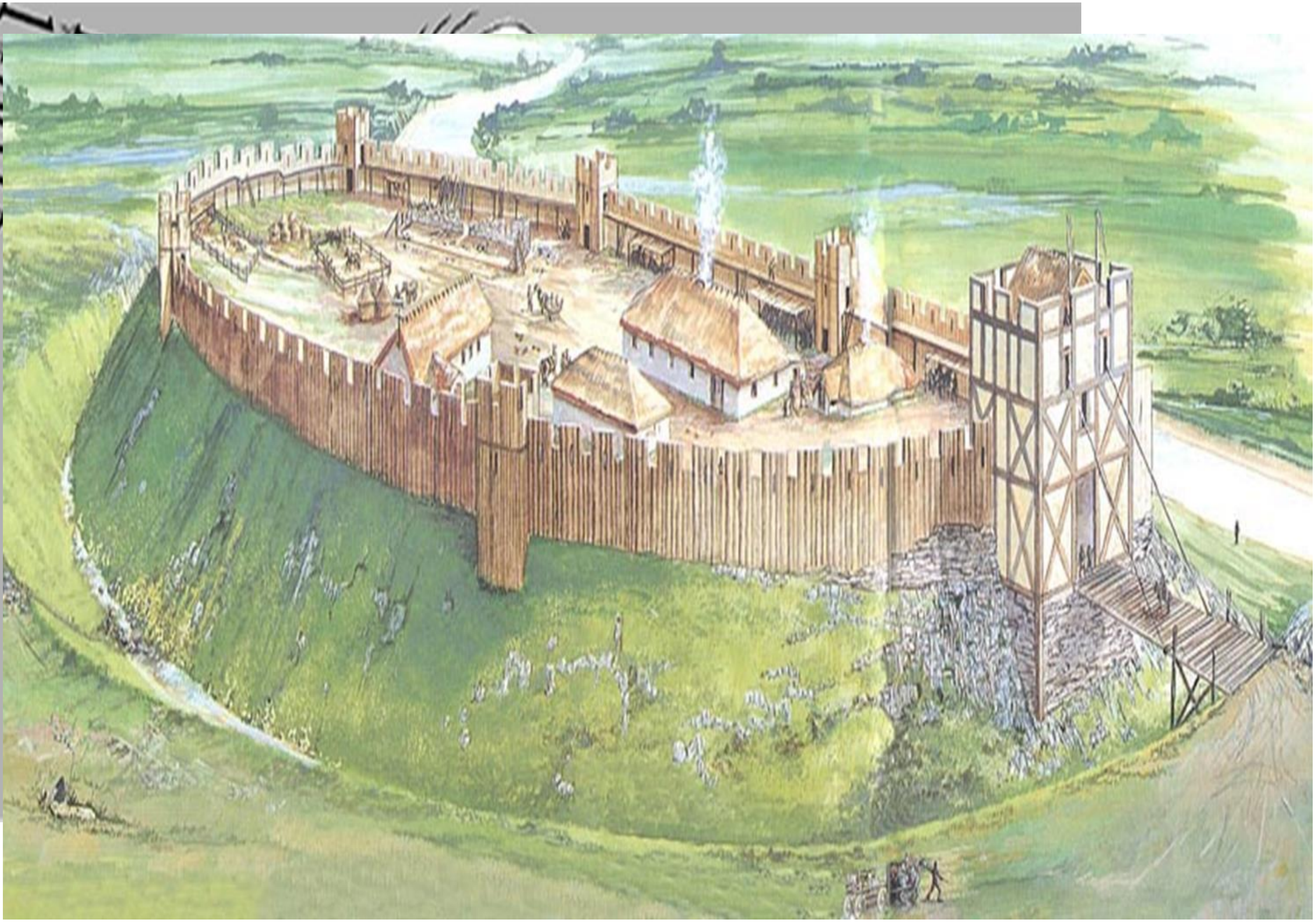
- Require individual user accounts for each employee

WE'RE SHARING A NETFLIX ACCOUNT NOW
SO I GUESS YOU COULD SAY THINGS ARE GETTING PRETTY SERIOUS
makeameme.org

IDENTIFY

- Create policies and procedures for information security

You shouldn't share your passwords either.
Be vigilant. Stay safe online.



PROTECT

- Limit employee access to data and information
- Install Surge Protectors and Uninterruptible Power Supplies (UPS)
- Patch your operating systems and applications
- Install and activate software and hardware firewalls on all your business networks

PROTECT

- Limit employee access to data and information

PROTECT

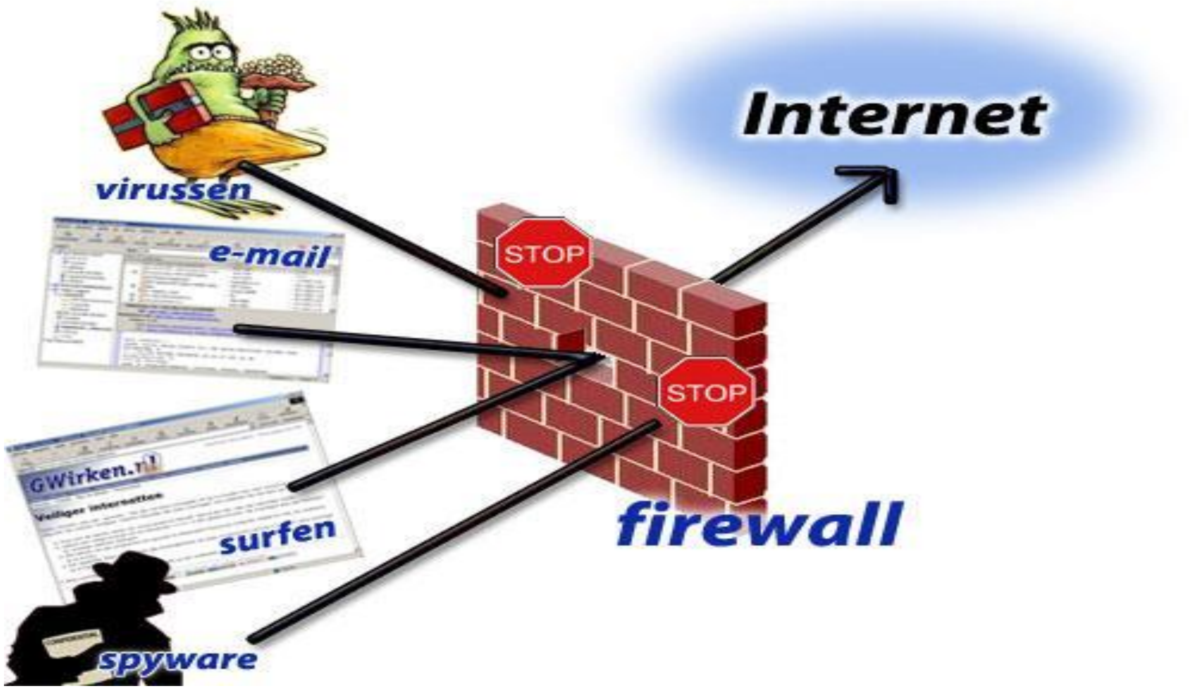
- Install Surge Protectors and Uninterruptible Power Supplies (UPS)

PROTECT

- Patch your operating systems and applications

PROTECT

- Install and activate software firewalls on all your networks
  - Software
  - Hardware



PROTECT (2)

- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

PROTECT (2)

- Secure your wireless access point and networks

© 2000 Randy Glasbergen. www.glasbergen.com

"WHEN YOU WANT TO GET SOMEBODY'S ATTENTION, THROW A ROCK AT HIS HEAD. IT'S THE LATEST THING IN WIRELESS COMMUNICATION!"

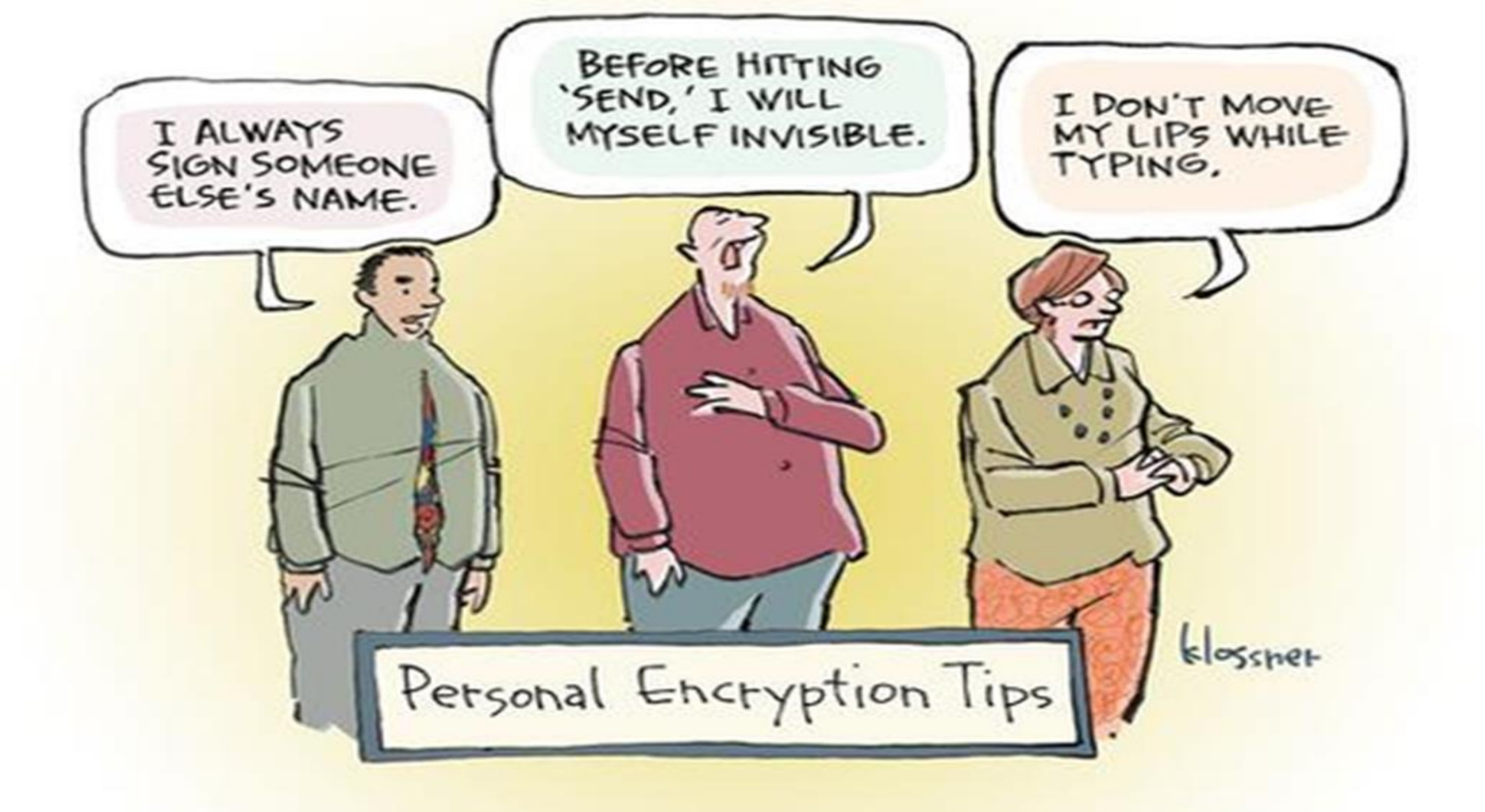
PROTECT (2)

- Set up web and email filters

"...and you spent 5.73 years of your life deleting spam from your e-mail."

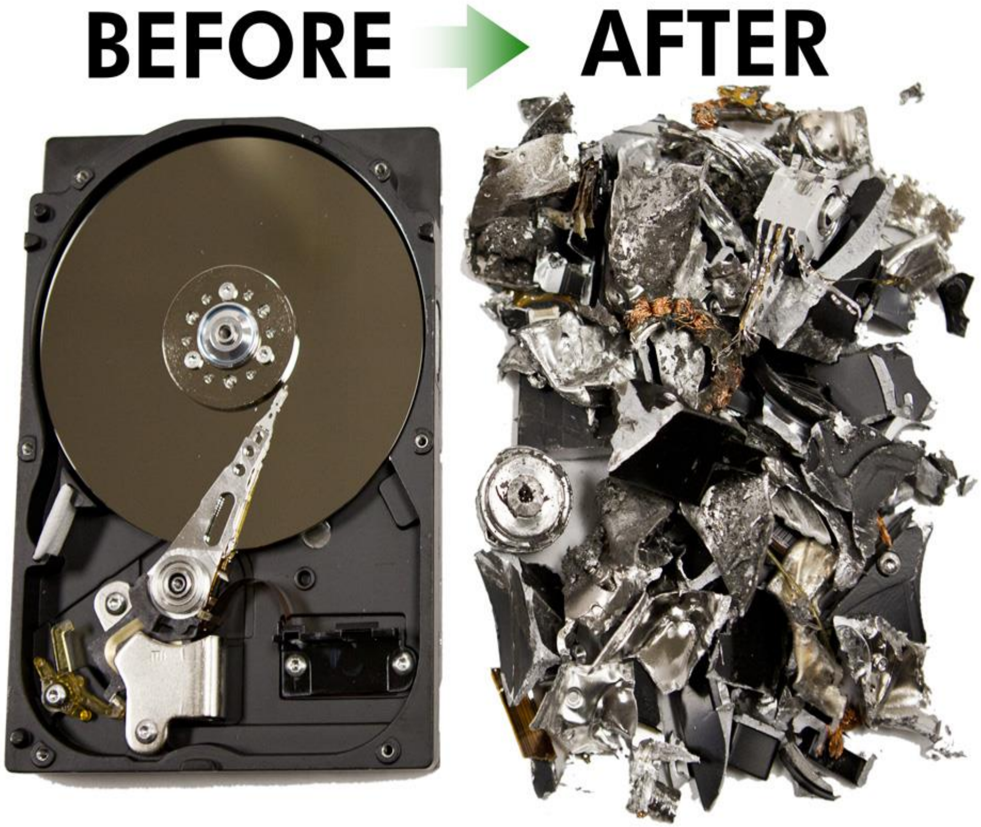
PROTECT (2)

- Use encryption for sensitive business information


I ALWAYS SIGN SOMEONE ELSE'S NAME.
'BEFORE HITTING 'SEND,' I WILL MYSELF INVISIBLE.
I DON'T MOVE MY LIPS WHILE TYPING.
Personal Encryption Tips
klossner

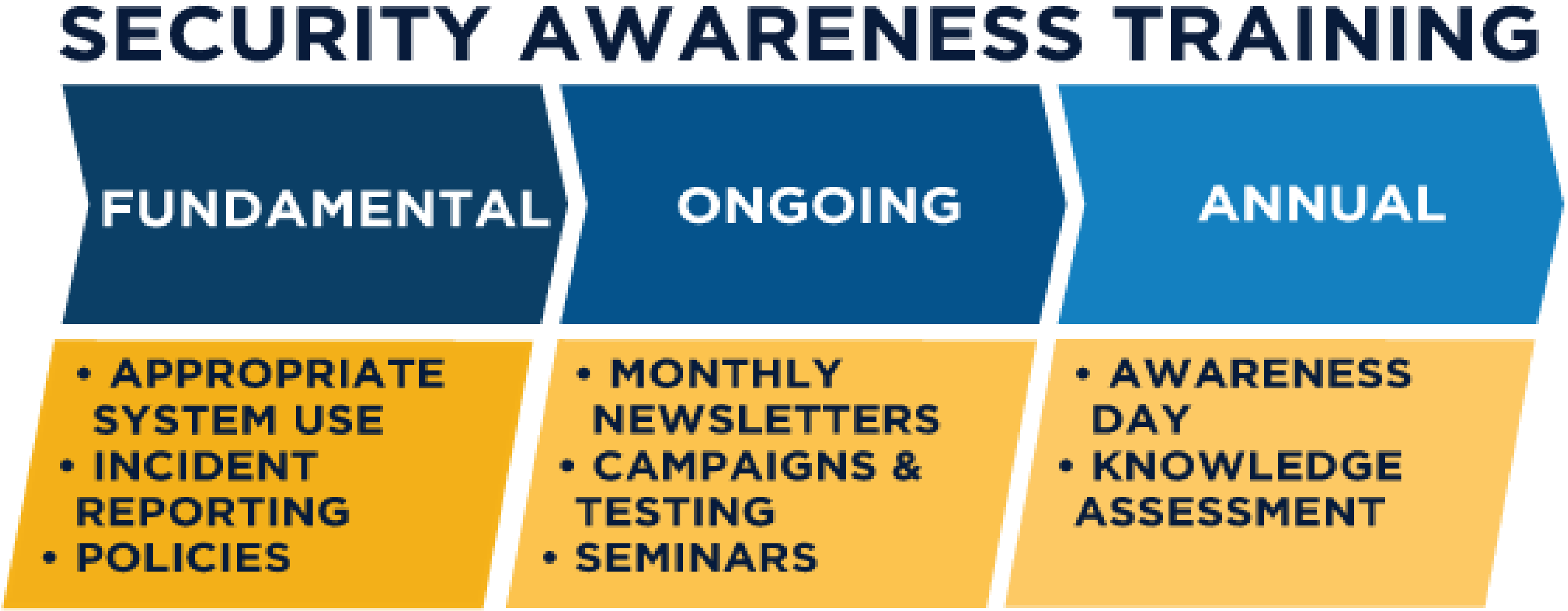
PROTECT (2)

- Dispose of old computers and media safely



PROTECT (2)

- Train your employees



SECURITY AWARENESS TRAINING

FUNDAMENTAL

- APPROPRIATE SYSTEM USE
- INCIDENT REPORTING
- POLICIES

ONGOING

- MONTHLY NEWSLETTERS
- CAMPAIGNS & TESTING
- SEMINARS

ANNUAL

- AWARENESS DAY
- KNOWLEDGE ASSESSMENT

DETECT

- Install and update
  - Anti-virus, Spyware, other malware programs

OUR COMPANY IS GOING TO MAKE ANTIVIRUS SOFTWARE. WHAT'S THAT TELL YOU?
IT TELLS ME WE'LL SECRETLY CREATE VIRUSES THAT CAN BE DETECTED ONLY BY OUR SOFTWARE.
AM I CLOSE?
YOU'RE SPOOKY.
www.dilbert.com
scottadams@aol.com
11-29-03 © 2003 United Feature Syndicate, Inc.
© UFS, Inc.

DETECT

- Maintain and monitor logs

RESPOND

- Develop a plan for disasters and information security incidents

RESPOND

- Develop a plan for disasters and information security incidents

OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...
HELP! HELP!
SOMEDAY WE HOPE TO HAVE A BUDGET.
www.dilbert.com scottadams@aol.com
8/15/00 © 2000 United Feature Syndicate, Inc.

RECOVER

- Make full backups of important business data/information
- Make incremental backups of important business data/information
- Consider cyber insurance
- Make improvements to processes / procedures / technologies

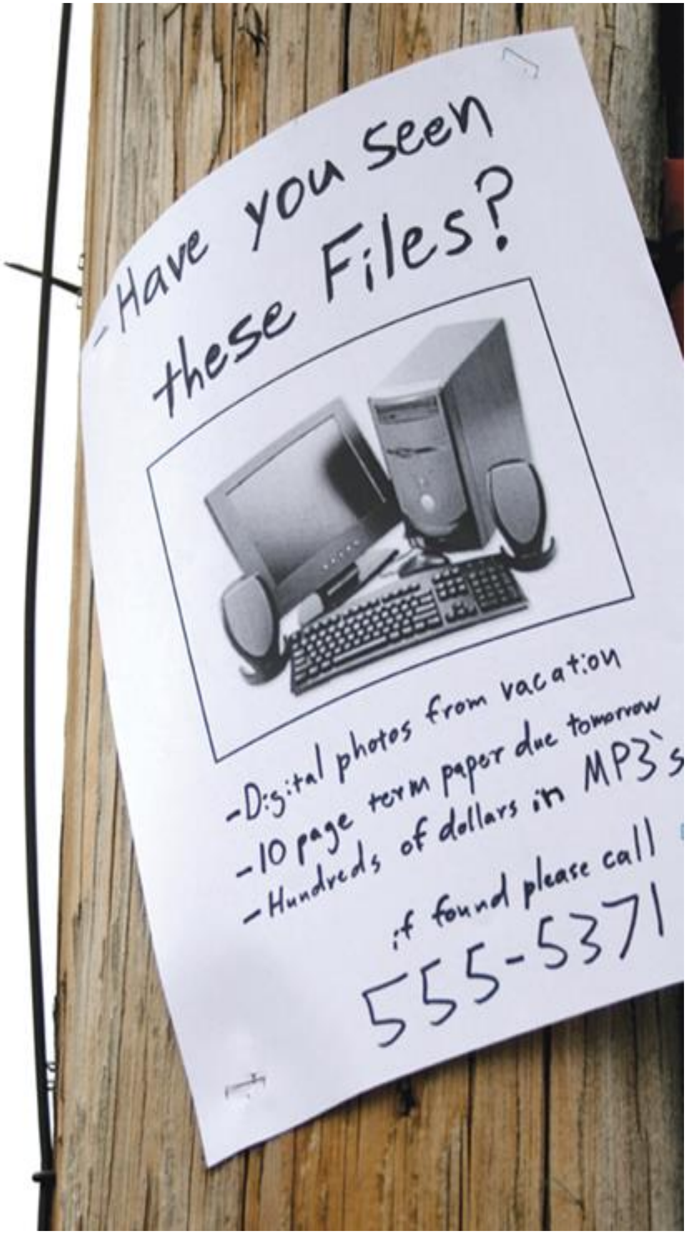
RECOVER

- Make full backups of important business data/information

I SHOULD WARN YOU ALL I MIGHT HAVE JUST CLICKED ON A LINK THAT MEANS WE SHOULD IMMEDIATELY SEEK ALTERNATIVE EMPLOYMENT

RECOVER

- Make incremental backups of important data/information


Have you seen these Files?
-Digital photos from vacation
-10 page term paper due tomorrow
-Hundreds of dollars in MP3's
if found please call
555-5371

RECOVER

- ➢Consider cyber insurance

Citizens can sue a county for failing to protect their data.

Knowing if your county has cybersecurity insurance and the specific coverage limits is crucial.

Counties need to secure a Certificate of Insurance evidencing cyber coverage from your vendors that perform IT services and payroll functions. This is not necessary for roofers or auto mechanics. One size does not fit all when it comes to certificates of insurance.

RECOVER

- Consider cyber insurance

The most important coverage features of a cyber policy are:

1) notification to advise citizens their PII may have been exposed;
2) ongoing credit monitoring; and
3) cyber extortion

The S.C. Property & Liability Trust cyber coverage provides for these three areas. *For specific coverage amounts or additional information, please contact Robert Collins, SCAC Director of Insurance Services, at rcollins@scac.sc or (803) 252-7255.*

Causes of Action

Plaintiff Demands

- Fraud reimbursement
- Credit card replacement
- Credit monitoring/ repair/ insurance
- Civil fines/ penalties
- Statutory damages (CMIA)
- Time
- Unjust enrichment
- Fear of ID Theft
- Actual ID Theft
- Mitigation costs
- Time spent monitoring

Protect your business with proper Cyber Liability coverage

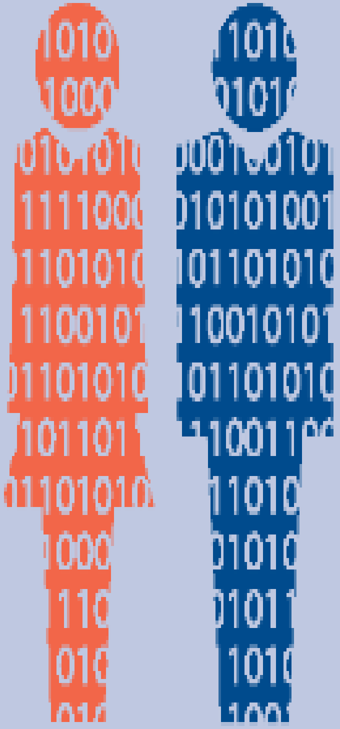
You need to protect your business against cyber hacks – those that directly impact your business and those that demonstrate a potential breach. Your insurance should cover:

- The cost to respond to a data breach
- Your legal defense and liability
- Your ID theft recovery expenses

SC CYBER

IT'LL **CO$T** YOU

2012 average cost per breach rose sharply to **$3.7 million - up 35%.**[4]



Legal costs are the largest portion of claims paid

Average cost of defense - **$582K**

Average cost of settlement - **$2.1 million**[4]

Information theft and business disruption represent the highest external costs

Information theft - **44%**

Disruption to business or lost productivity - **30%**[1]

Cyber crime costs small organizations more – they incur a significantly higher per capita cost than larger organizations[1]

SC CYBER

Montana’s Cyber Risk Insurance

- Montana participates in a national cyber/information security insurance program underwritten by Certain Underwriters at Lloyd’s, Syndicators 623 and 2623 (“Beazley”).
- $2,000,000 Policy Aggregate Limit for Privacy Notification Costs (subject to a $100,000 per incident Retention); $1,000,000 Policy Aggregate Limit for Beazley Nominated Service Providers.
- Insurance doesn’t cover everything. $100,000 deductible, 10% state co-insurance for credit monitoring.
- Coverage is nice, but breach prevention should be the collective focus.

Montana’s Cyber Risk Insurance

The state’ s commercial insurance policy provides coverage for:

•Data breach response costs including, but not limited to, forensic investigations, mail notification, and credit monitoring (one year).

•Fines/penalties assessed by regulatory authorities.

•Revenue streams lost as a result of a breach.

•Personal injuries and property damage for negligent acts or omissions of the state.

•Website content and media.

•Cyber ransoms and fines.

•Public relations firm consultation

Montana’s Cyber Risk Insurance

Annual Renewal Information:

- IT Security Audit completion – date of last audit
- Penetration Testing - date of last test
- Encryption of sensitive information physically removed from state offices
- Number of records with personally identifiable information
- Security Training and Awareness Program
- Report of any incidents that have resulted in claims.

Cyber Incident Response Process
Step One: Notify Response Team

- Use the term “incident” instead of “breach” as a point of reference in all communications.
- Notify your agency’s internal incident response team (i.e. agency head, IT manager, risk manager, attorney, etc.).
- Notify the cyber insurance brokerage firm and cyber insurance carrier.
- Follow the instructions found at the Risk Management & Tort Defense Division’s (RMTD) website at http://rmtd.mt.gov/claims/agenciesreportclaims.mcpx
  - Ø Call us within 24 hours at (406) 444-2421
  - Ø Have the immediate supervisor complete the “Report of Incident” and send it to us within two days.
  - Ø Do not contact individuals whose information may have been released. Do not contact law enforcement or regulatory authorities

Cyber Incident Response Process
Step Two: Escalate as Necessary

- Internal investigation and reporting of incident to the State ' s cyber liability insurance carrier;
- Privacy counsel (attorney-client privilege and work product protections);
- Computer forensics expert;
- Public relations and crisis management consultant;
- Mailing/notification vendor (is your agency equipped to print and mail 5,000 notification letters? How about 50,000? 500,000?);
- **Timing is everything:** Notification (to the affected individuals) must be made **without unreasonable delay**, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. Mont. Code Anno., § 2-6-504(1)(b)
- Fixed deadlines in other states

Case Study

DPHHS 2014 Cyber Incident Timeline

- May 15th – Initial discovery
- May 22nd – Forensic confirmation
- May 29th – Initial public communication
- June 23rd – File sent to mail processing center (1.3M)
- June 24th – Follow-up public communication
- July 3rd – Began mailing - 200K notices/day

DPHHS 2014 Cyber Incident - HIPAA Clock

- On complex security issues, the key timeframe of notification is the 60-day HIPPA requirement, which begins with initial discovery
- Performed scope analysis of incident
- Created notification list
- Documented potential HIPAA exposure for Office of Civil Rights

DPHHS Message to Public/Press (cont.)

- **How did this happen?** Unknown computer hackers used malware to gain entry to a DPHHS server containing client and agency employee personal information.
- **Have those affected clients been notified?** At this time, DPHHS is in the process of notifying all those people with information on the server.
- **What type of security is in place on the server?** We are continuously working to improve security of our computer networks and are committed to protecting client information. We deeply regret any inconvenience to you as a result of this incident. To help prevent something like this from happening in the future, we have taken the affected server offline and a new server containing backup files is being scanned and safely brought online. DPHHS has purchased additional security software to better protect sensitive information on existing servers, and as part of an internal investigation, DPHHS is reviewing existing policies and procedures to determine how to prevent this from happening again in the future.
- **Will this affect the services I receive?** This incident should not impact DPHHS services as none of the information contained on the server was lost and we have a complete back-up of the information.

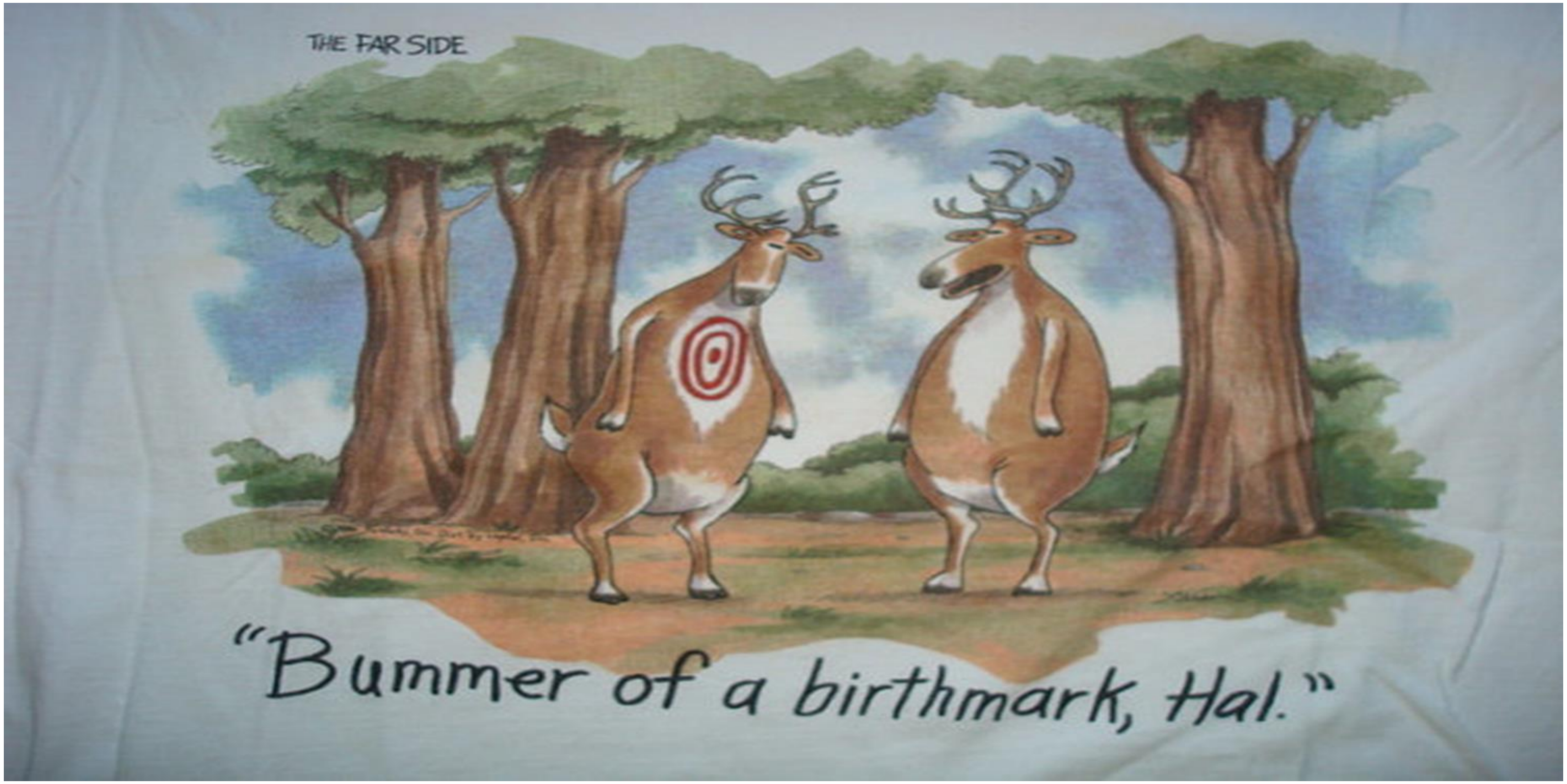
Montana’s Cyber Risk Insurance

What was provided during the 2014 HHS Incident:

- Forensic investigation
- Public relations consultation
- Legal consultation
- Website content recommendations - FAQs
- Recommendation on all communication internal and external
- mail notification
- credit monitoring (one year)
- Call center for 60 days

RECOVER

- Make improvements to processes / procedures / technologies



2018 cybersecurity outlook for SLTT governments

- Cybercrime against SLTT governments will again be motivated primarily by financial gain.
- Network boundaries will be broken as new cybercrime will increasingly target apps, cloud computing, Internet of Things, cryptocurrencies and supply chain.
- Cybersecurity workforce demand will climb and likely outpace supply. SLTT governments will have a hard time competing with private sector salaries and drawing qualified workers.
- New technology (body cameras, drones, apps) will continue to change how chief information security officers do their jobs.

MS-ISAC™

Multi-State Information Sharing & Analysis Center®

NATIONWIDE CYBER SECURITY REVIEW

NACO National Association of Counties

The Voice of America's Counties

NASCIO

Representing Chief Information Officers of the States

Testimonial

“The NCSR provides a unique perspective on your security maturity as a snapshot of your program against the NIST Cybersecurity Framework. It provides valuable insights in measuring your security program while giving you annual comparatives of growth and peer-to-peer analysis!   Well worth over $60K to any organization in helping to roadmap your security operation!”

-----Gary Coverdale, CISO-Mono County

How Did We Get Here?

- In June of 2009, the Department of Homeland Security (DHS) was directed to develop a cyber-network security assessment to measure state, local, tribal and territorial (SLTT) governments' gaps and capabilities
- The first Nationwide Cybersecurity Review (NCSR) was conducted in 2011 by DHS
- In 2013, DHS partnered with the MS-ISAC, the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop and conduct the second NCSR
- Since 2013, the NCSR has been conducted on an annual basis
- 2017 marks the 6th year the self-assessment has been conducted
- In 2015, the NCSR was aligned to the NIST CSF

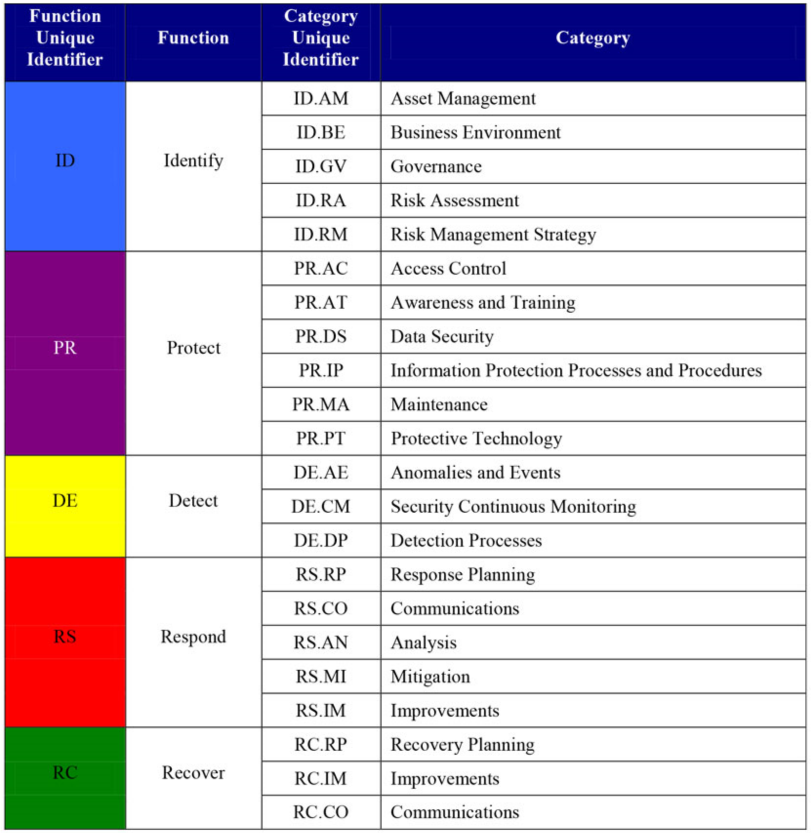
About the Nationwide Cyber Security Review

The Nationwide Cyber Security Review (NCSR) is a free, confidential, annual self-assessment survey that is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by the Department of Homeland Security (DHS) and the MS-ISAC.

The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial (SLTT) governments.

Using the results of the NCSR, DHS delivers a biyearly anonymous summary report to Congress providing a broad picture of the cybersecurity maturity across the SLTT communities.

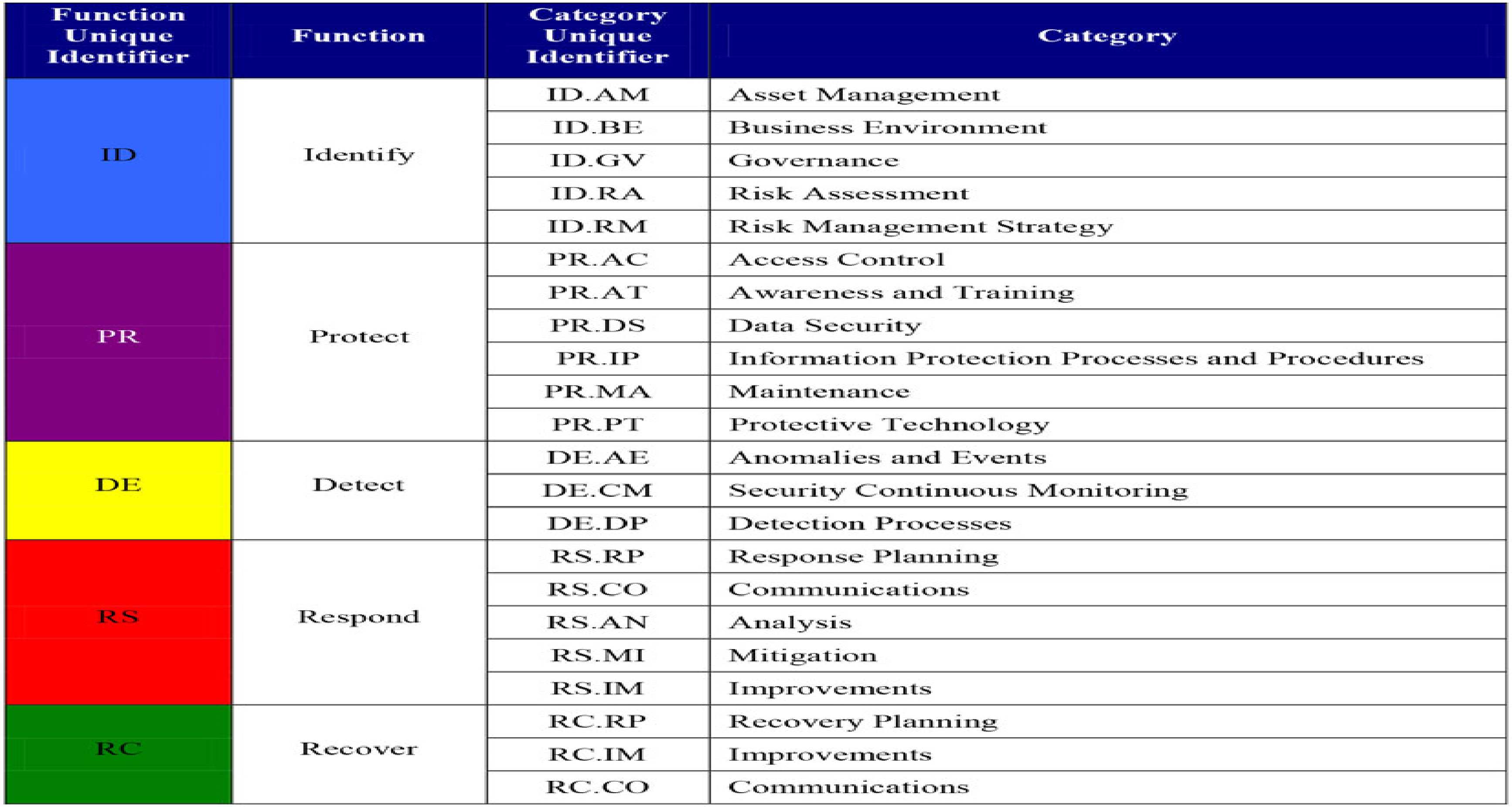
Cybersecurity Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

About the Nationwide Cyber Security Review

Cybersecurity Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Why Participate in the NCSR?

- Receive metrics specific to your organization
- Develop a benchmark to gauge your year-to-year progress
- Use the metrics to identify gaps in your security program
- Anonymously measure your results against your peers
- Access to NIST, COBIT, ISO and CIS Controls informative references
- For HIPAA compliant agencies, translates your NCSR scores to the HIPAA Security Rule scores for an automatic self-assessment tool
- Be a part of the ongoing effort to chart national cybersecurity maturity and identify areas of concern
- Aligned with the Presidential Executive Order on Strengthening Cybersecurity (NIST CSF)

Available NCSR Reports

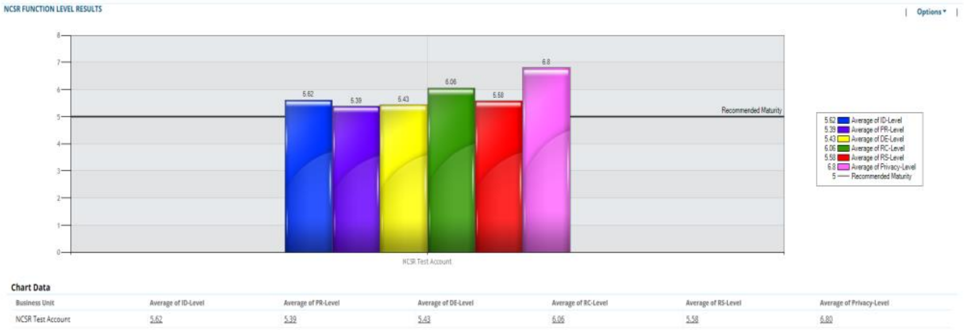


Chart Data

Business Unit	Average of ID-Level	Average of PR-Level	Average of DE-Level	Average of RC-Level	Average of RS-Level	Average of Privacy-Level
NCSR Test Account	5.62	5.39	5.43	6.06	5.58	6.80

This report provides your organizations CSF function averages.

Reports that provide informative references such as: Critical Security Controls, NIST 800-53 & COBIT for any control that does not meet the recommended minimum maturity of “Implementation in Process” or “Risk Formally Accepted”.

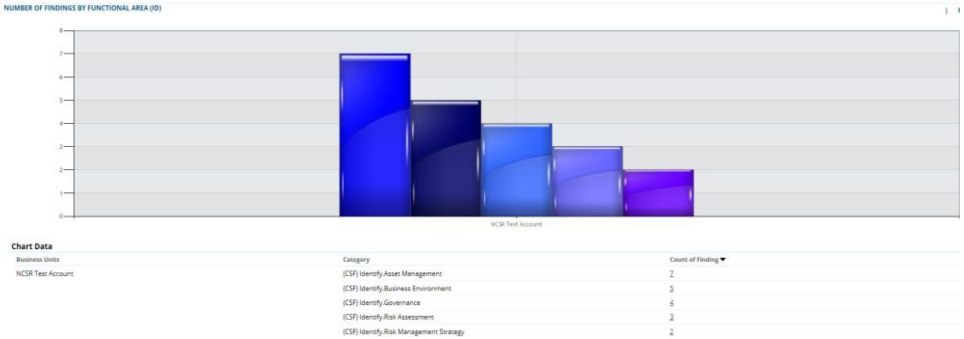


Chart Data

Business Units	Category	Count of Finding ▼
NCSR Test Account	(CSF) Identify.Asset Management	7
	(CSF) Identify.Business Environment	5
	(CSF) Identify.Governance	4
	(CSF) Identify.Risk Assessment	3
	(CSF) Identify.Risk Management Strategy	2

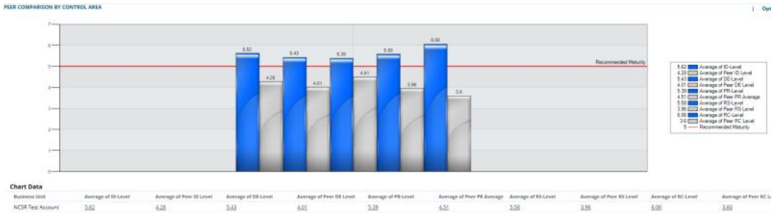


Chart Data

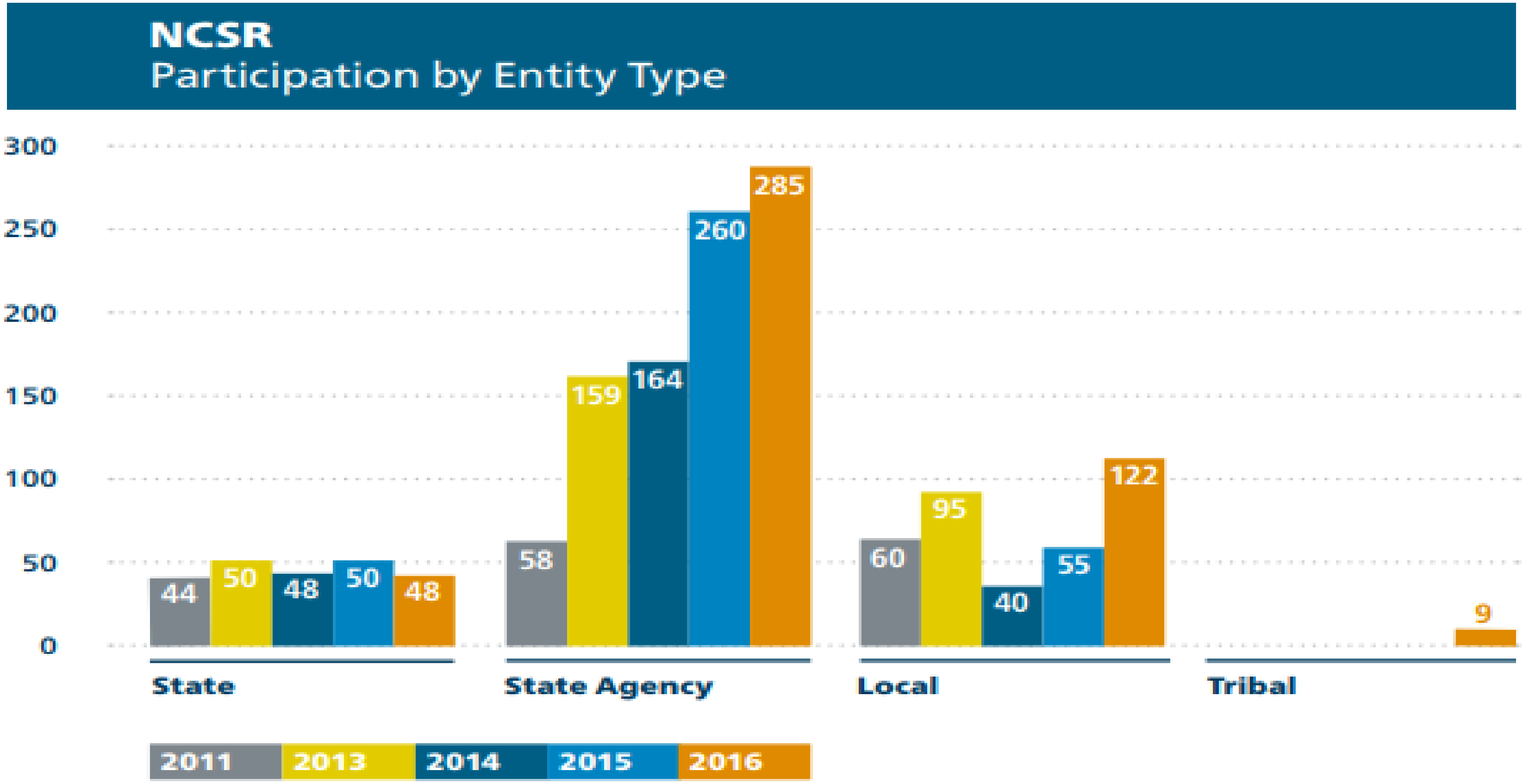
Business Unit	Average of ID-Level	Average of Peer ID Level	Average of DE-Level	Average of Peer DE Level	Average of PR-Level	Average of Peer PR Average	Average of RS-Level	Average of Peer RS Level	Average of RC-Level	Average of Peer RC L
NCSR Test Account	5.62	4.28	5.43	4.01	5.39	4.51	5.58	3.96	6.06	3.60

Peer-to-peer reports compare your results to your peers.

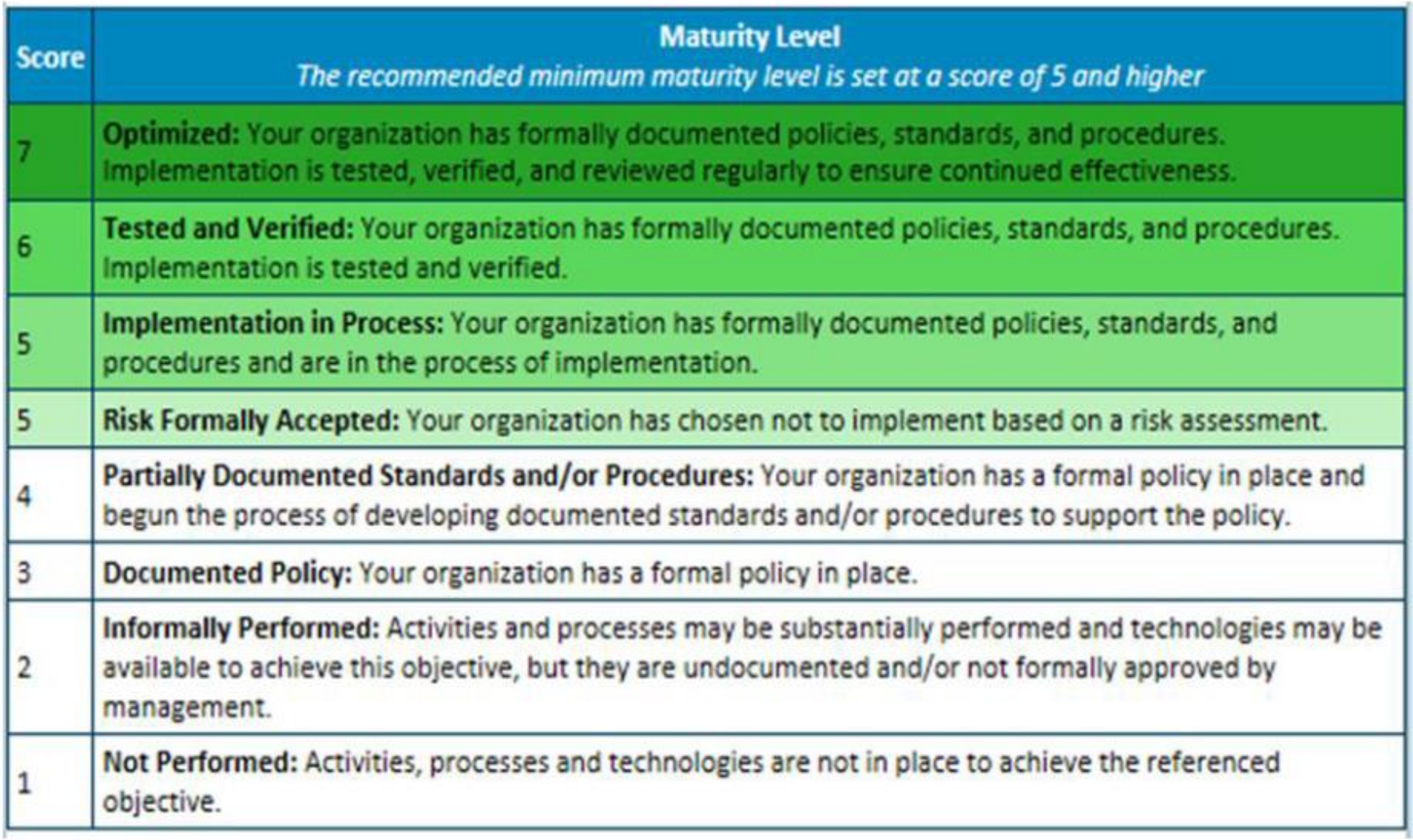
How Are Organizations Using the NCSR?

1. To see how their organization rates compared to similar organizations (peer to peer reports)
2. To inform C-level/executive management about security programs/resources needs
3. Establish priorities for program tasks
4. Improved understanding of your cybersecurity posture & capabilities

NCSR Yearly Participation

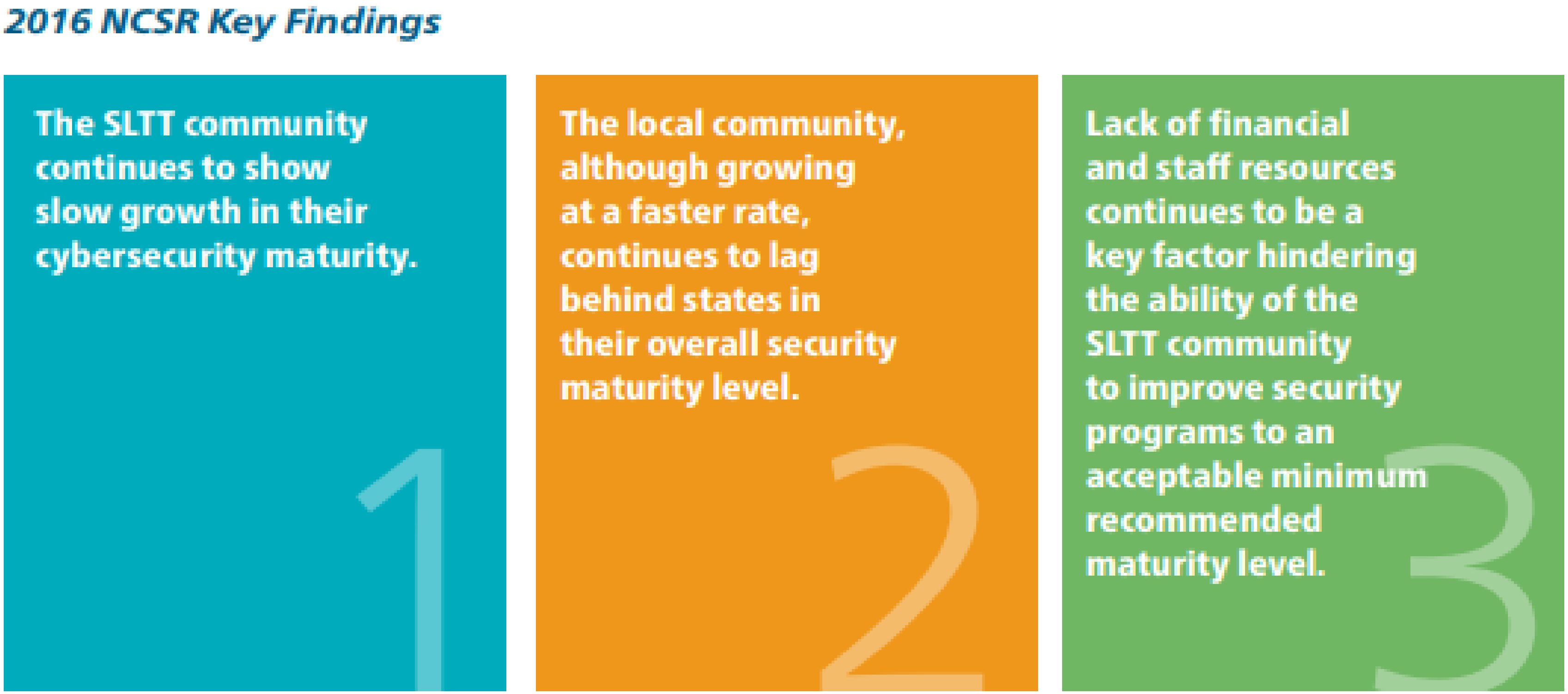


Response Scale



Score	**Maturity Level** *The recommended minimum maturity level is set at a score of 5 and higher*
7	**Optimized:** Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:** Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:** Your organization has formally documented policies, standards, and procedures and are in the process of implementation.
5	**Risk Formally Accepted:** Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:** Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:** Your organization has a formal policy in place.
2	**Informally Performed:** Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:** Activities, processes and technologies are not in place to achieve the referenced objective.

2016 Key Findings



2016 NCSR Key Findings

1. The SLTT community continues to show slow growth in their cybersecurity maturity.

2. The local community, although growing at a faster rate, continues to lag behind states in their overall security maturity level.

3. Lack of financial and staff resources continues to be a key factor hindering the ability of the SLTT community to improve security programs to an acceptable minimum recommended maturity level.

2016 Summary Report Highlights

The following trends were identified within the local and state peer profiles:

- State governments continue to be weakest in the Identify Function and the strongest in the Respond Function.
- Local governments continue to be weakest in the Detect Function and strongest in the Protect Function.
- Tribal governments are similar to local governments in that they are strongest in the Protect Function.
- The Detect Function continues to represent the largest maturity gap between state and local governments.

- **State governments** continue to remain more mature than the rest of the SLTT community
- **State and local respondents** identified insufficient funding along with increased sophistication of threats as top cybersecurity concerns.
- **State and local governments** continue to improve their overall cybersecurity maturity despite operating in an environment of sophisticated threats and attacks.

NATIONWIDE CYBER SECURITY REVIEW

SC CYBER

MS-ISAC

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments.

Our Membership

Members include:

- All 50 states & Territories
- All 78 DHS-recognized Fusion Centers
- Over 1,100 Local and Tribal governments (representing over 48% of the U.S. population)

State, Local, Tribal, and Territorial

departments, cities, towns, police department, ports, airports, schools, transit associations, and more

24x7 Security Operations Center

Central location to report any cyber security incident

24/7 support for:

- ✓ Network Monitoring Services
- ✓ Research and Analysis

24/7 analysis and monitoring of:

- ✓ Threats
- ✓ Vulnerabilities
- ✓ Attacks

24/7 reporting:

- ✓ Cyber Alerts & Advisories
- ✓ Web Defacements
- ✓ Account Compromises
- ✓ Hacktivist Notifications

24 / 7 / 365 Monitoring & analysis of ~100 billion logs

__Phone__: 1-866-787-4722

__Email__: soc@msisac.org

Monitoring of IP Range & Domain Space

IP Monitoring

✓IPs connected to a particular malicious C&C

✓Compromised IPs

✓Indicators of compromise from the MS-ISAC network monitoring system (Albert)

✓Notifications from Spamhaus

Domain Monitoring

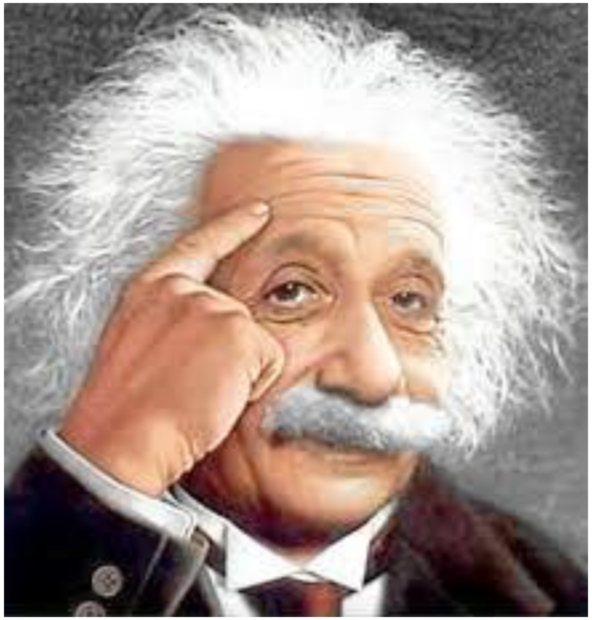
✓Notifications on compromised user credentials

✓Vulnerability Management Program (VMP)

TLP: WHITE

Network Monitoring (Albert)

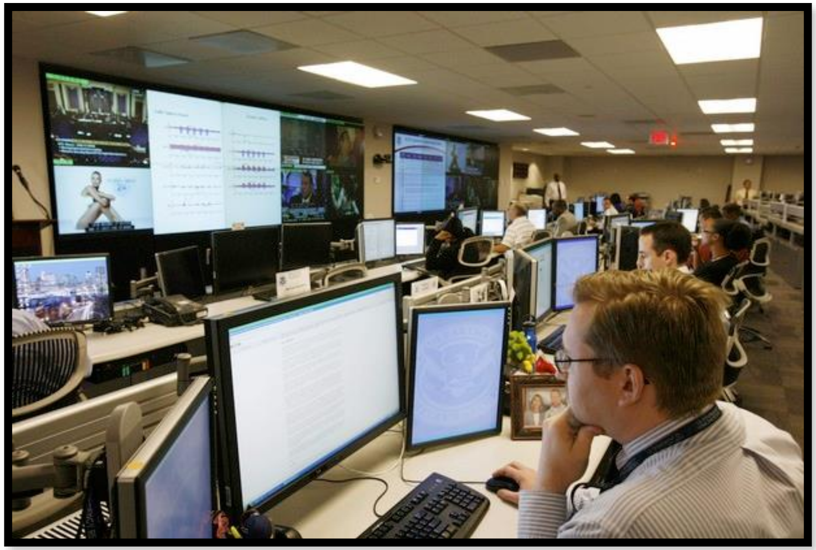
- ✓SLTT focus
- ✓24x7x365 research, analysis, and support
- ✓Signatures unique to SLTT governments
- ✓Integration of research on specific attacks and actors, including nation-state actors (APT)
- ✓Real-time information sharing with SLTT partners
- ✓Experienced cybersecurity analysts who review each event minimizing the number of false-positive notifications



TLP: WHITE

MS-ISAC Intelligence Sources

- 24x7 Monitoring
  - Analysis of 60 billion logs/records per week
- Intelligence Partners
- Federal Government
  - NCCIC
- Private Sector
- Internet Research



Computer Emergency Response Team

CERT Capabilities

- Incident Response (includes on-site assistance)
- Malware Analysis
- Computer & Network Forensics
- Network & Web Application Vulnerability Assessments
- Log Analysis
- Netflow Monitoring/Albert
- Penetration Testing

Vulnerability Management Program

Any SLTT government agency or department may participate.

What You Get:

- Victim Notifications when that domain/IP is observed in a malicious context (e.g. data dumps, sending spam, etc.)
- Website Vulnerability Review that checks to ensure you have the most up to date software on your website

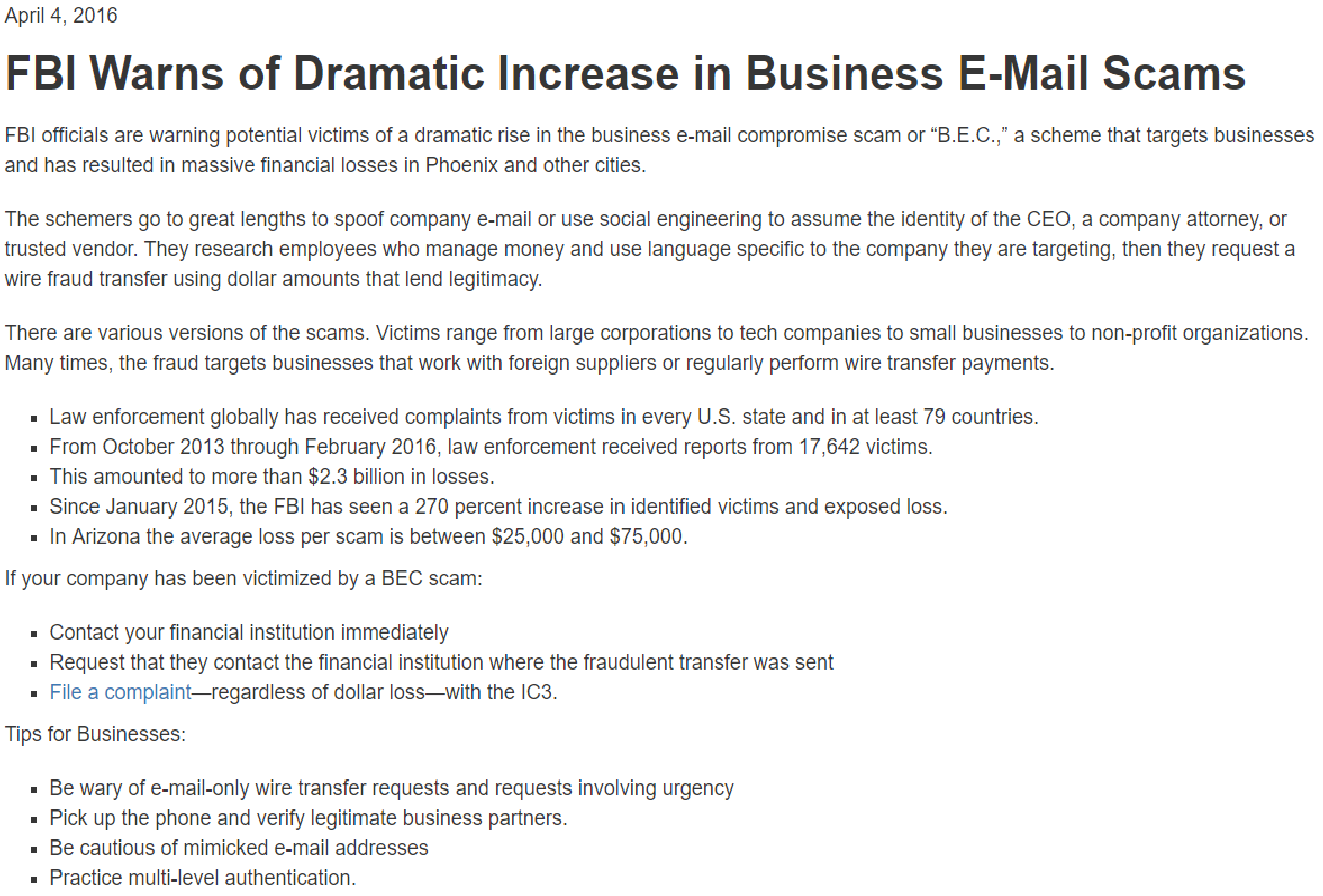
What We Need:

- **Domains**
- **IP ranges**
- **Contact info** (name, email, phone number)

Send to VMP@cisecurity.org

Member Services

- Access to US CERT Portal/HSIN
- Access to the Malicious Code Analysis Platform
- National Cyber Security Review
- Seven Member Work Groups
- Monthly Newsletters for End Users
- Monthly Member Calls
- Monthly Situational Awareness Reports
- Cyber Exercises
- Annual Meeting



April 4, 2016

FBI Warns of Dramatic Increase in Business E-Mail Scams

FBI officials are warning potential victims of a dramatic rise in the business e-mail compromise scam or "B.E.C.," a scheme that targets businesses and has resulted in massive financial losses in Phoenix and other cities.

The schemers go to great lengths to spoof company e-mail or use social engineering to assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money and use language specific to the company they are targeting, then they request a wire fraud transfer using dollar amounts that lend legitimacy.

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

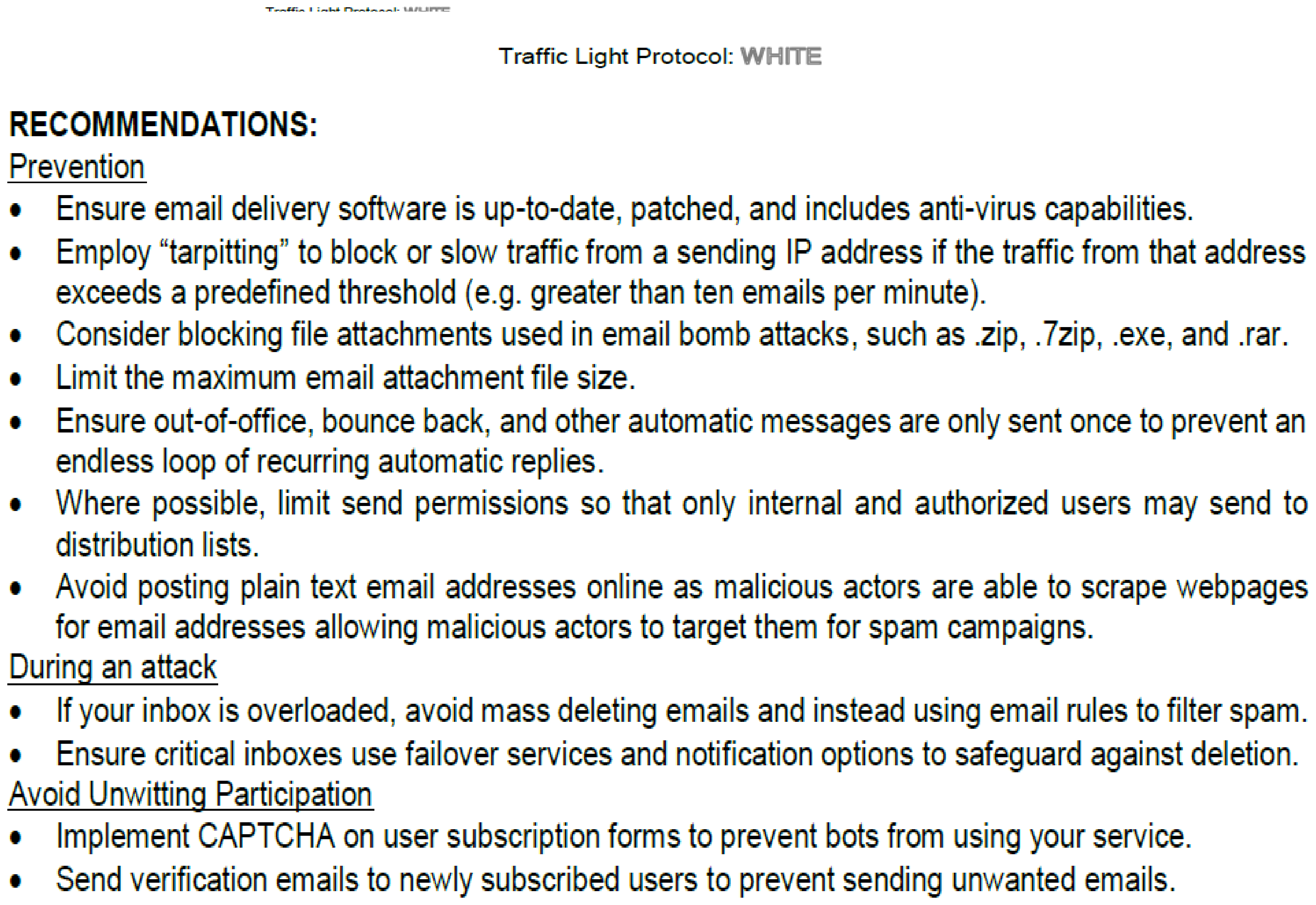
- Law enforcement globally has received complaints from victims in every U.S. state and in at least 79 countries.
- From October 2013 through February 2016, law enforcement received reports from 17,642 victims.
- This amounted to more than $2.3 billion in losses.
- Since January 2015, the FBI has seen a 270 percent increase in identified victims and exposed loss.
- In Arizona the average loss per scam is between $25,000 and $75,000.

If your company has been victimized by a BEC scam:

- Contact your financial institution immediately
- Request that they contact the financial institution where the fraudulent transfer was sent
- File a complaint—regardless of dollar loss—with the IC3.

Tips for Businesses:

- Be wary of e-mail-only wire transfer requests and requests involving urgency
- Pick up the phone and verify legitimate business partners.
- Be cautious of mimicked e-mail addresses
- Practice multi-level authentication.



Traffic Light Protocol: WHITE

RECOMMENDATIONS:

Prevention

- Ensure email delivery software is up-to-date, patched, and includes anti-virus capabilities.
- Employ “tarpitting” to block or slow traffic from a sending IP address if the traffic from that address exceeds a predefined threshold (e.g. greater than ten emails per minute).
- Consider blocking file attachments used in email bomb attacks, such as .zip, .7zip, .exe, and .rar.
- Limit the maximum email attachment file size.
- Ensure out-of-office, bounce back, and other automatic messages are only sent once to prevent an endless loop of recurring automatic replies.
- Where possible, limit send permissions so that only internal and authorized users may send to distribution lists.
- Avoid posting plain text email addresses online as malicious actors are able to scrape webpages for email addresses allowing malicious actors to target them for spam campaigns.

During an attack

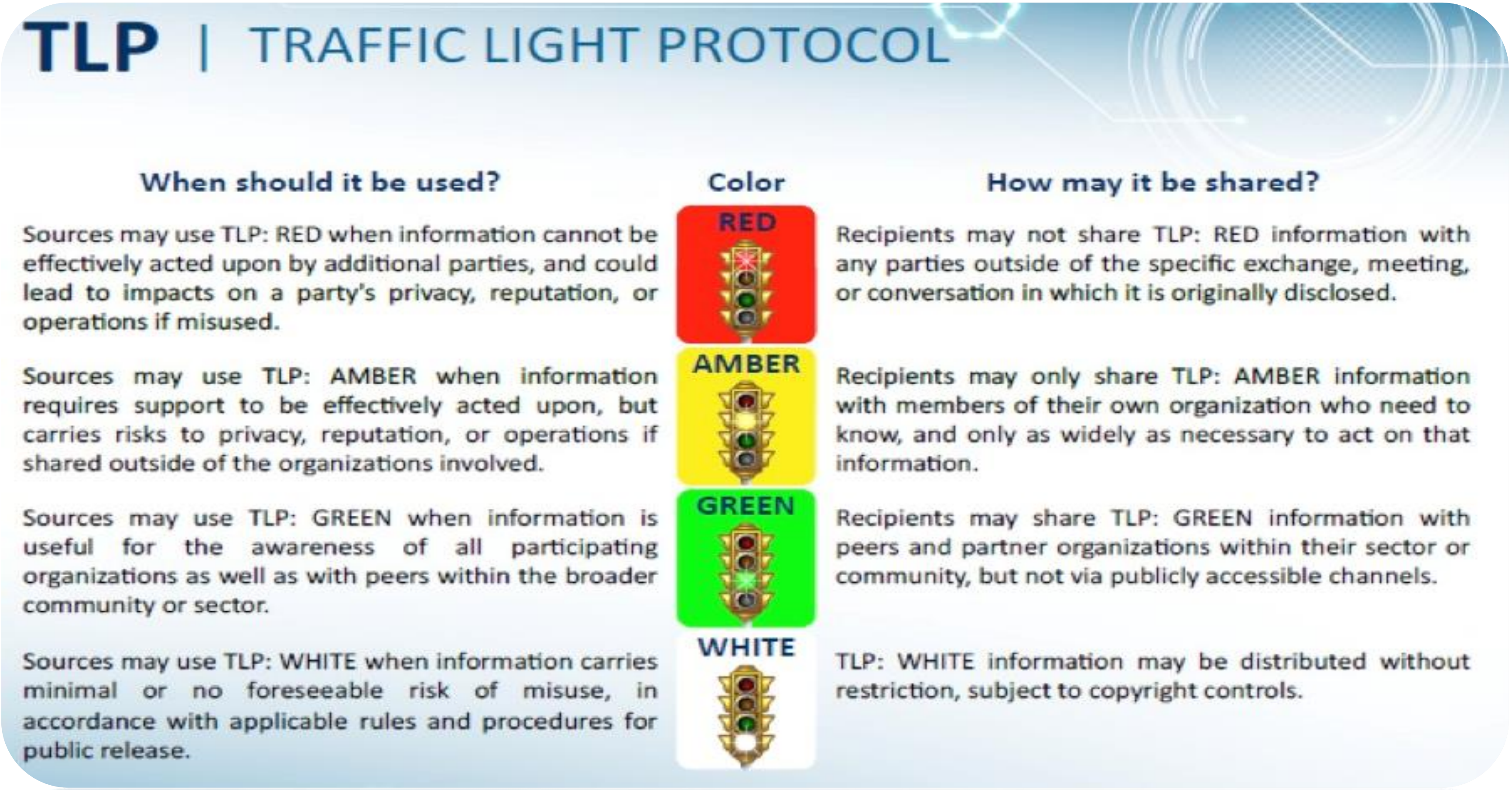
- If your inbox is overloaded, avoid mass deleting emails and instead using email rules to filter spam.
- Ensure critical inboxes use failover services and notification options to safeguard against deletion.

Avoid Unwitting Participation

- Implement CAPTCHA on user subscription forms to prevent bots from using your service.
- Send verification emails to newly subscribed users to prevent sending unwanted emails.

Traffic Light Protocol (TLP)

All correspondence will have a predetermined TLP rating defining the way that information can be shared.



TLP | TRAFFIC LIGHT PROTOCOL

When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Contact Information

Secure Operations Center/CERT

24/7 Phone Number
1-866-787-4722
soc@msisac.org

MS-ISAC Headquarters

Main Line
518-266-3460
info@msisac.org

www.msisac.cisecurity.org

SC CYBER

"SC Cyber is an opportunity to build a cyber ecosystem that leverages the best of industry, academia, and government. By utilizing 21st century technologies, tools, and talents, we can improve the security and prosperity of our state and our region."

– LES EISNER, USC OFFICE OF ECONOMIC ENGAGEMENT

SC CYBER

What is SC Cyber?

Announced February 2016

"…what we have to remember is those who attack are patient, and those that attack never stop trying.

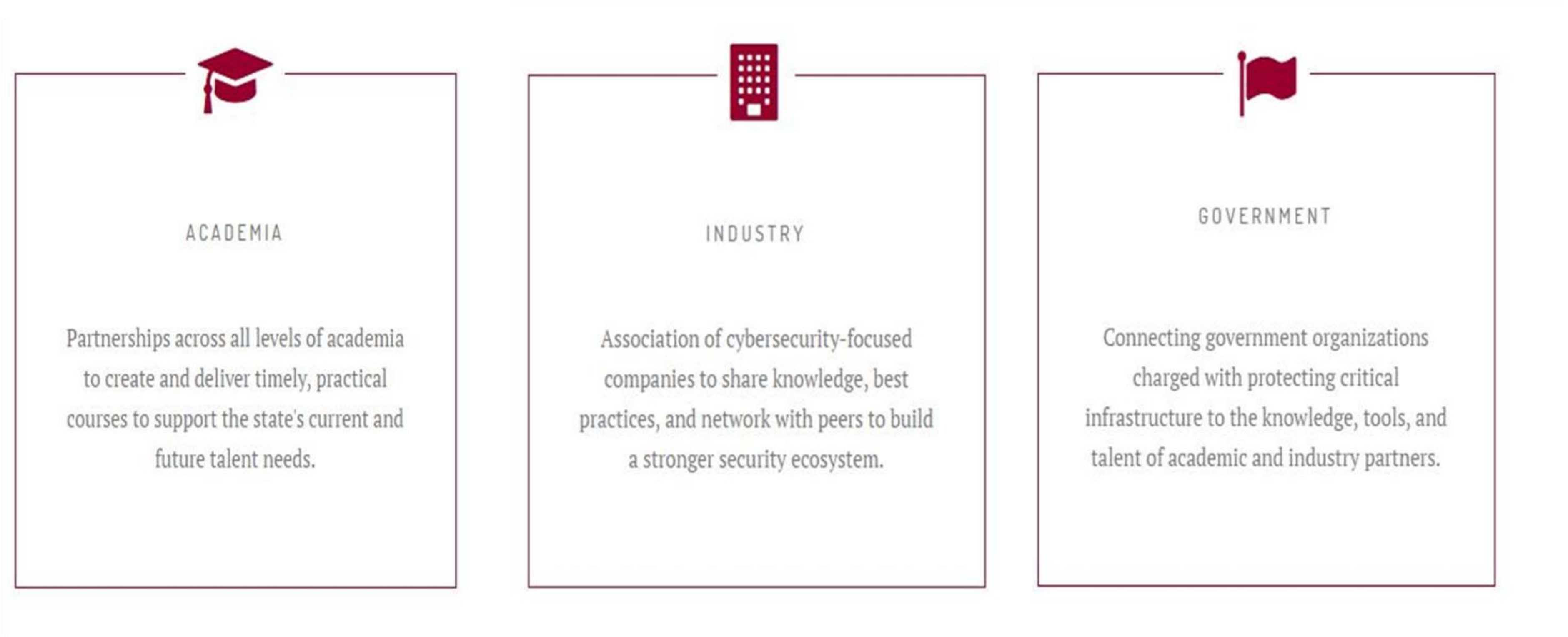
So if that's the case, we can never stop working to make sure we keep things safe."

-- Governor Nikki Haley

SC CYBER

What is SC Cyber?

Statewide initiative with partners across all levels of academia, industry, and government



ACADEMIA

Partnerships across all levels of academia to create and deliver timely, practical courses to support the state's current and future talent needs.

INDUSTRY

Association of cybersecurity-focused companies to share knowledge, best practices, and network with peers to build a stronger security ecosystem.

GOVERNMENT

Connecting government organizations charged with protecting critical infrastructure to the knowledge, tools, and talent of academic and industry partners.

Areas of Focus

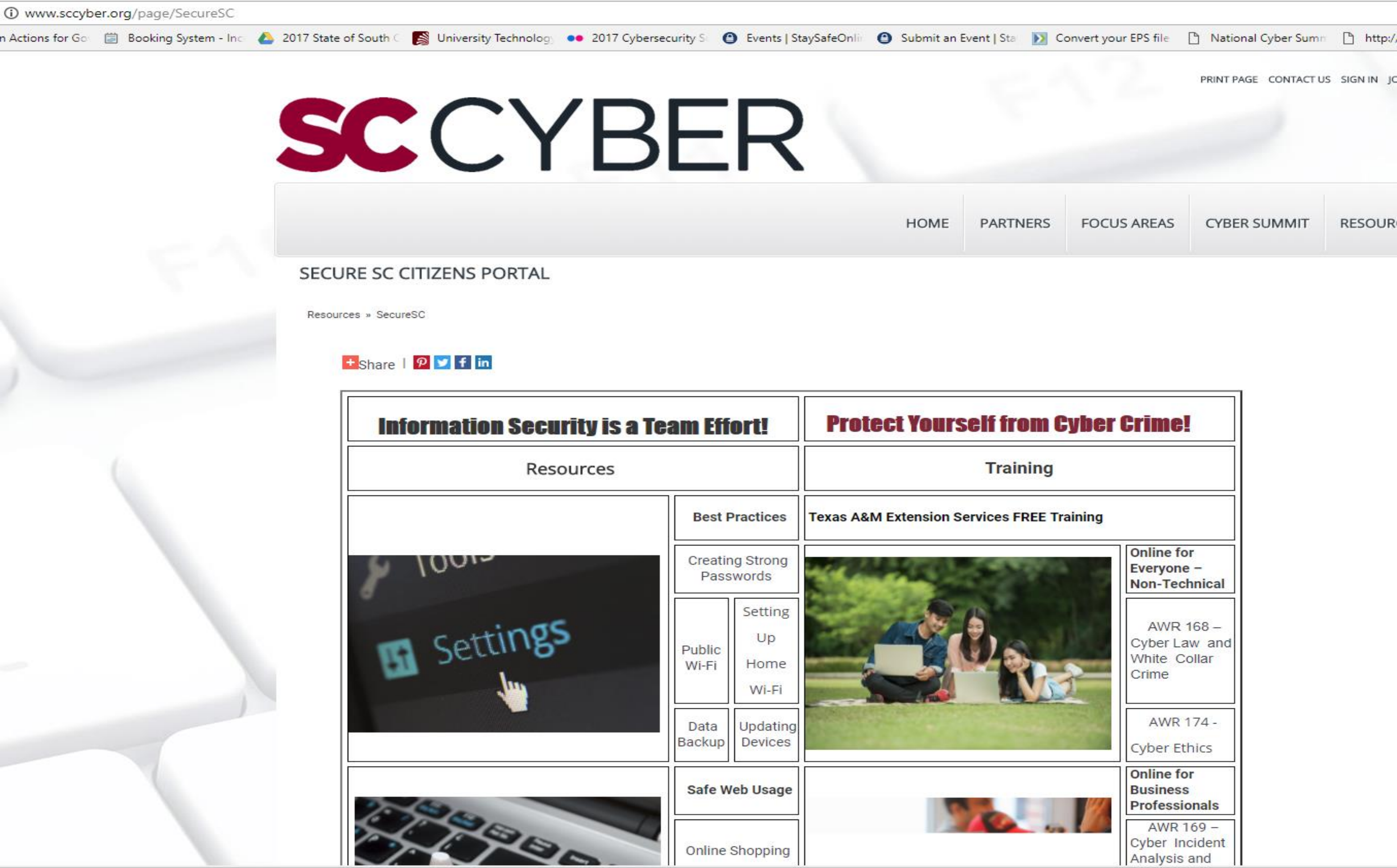
Education

Protection

Research

Workforce Development

Knowledge Management



www.sccyber.org/page/SecureSC

PRINT PAGE CONTACT US SIGN IN JC

SC CYBER

HOME PARTNERS FOCUS AREAS CYBER SUMMIT RESOUR

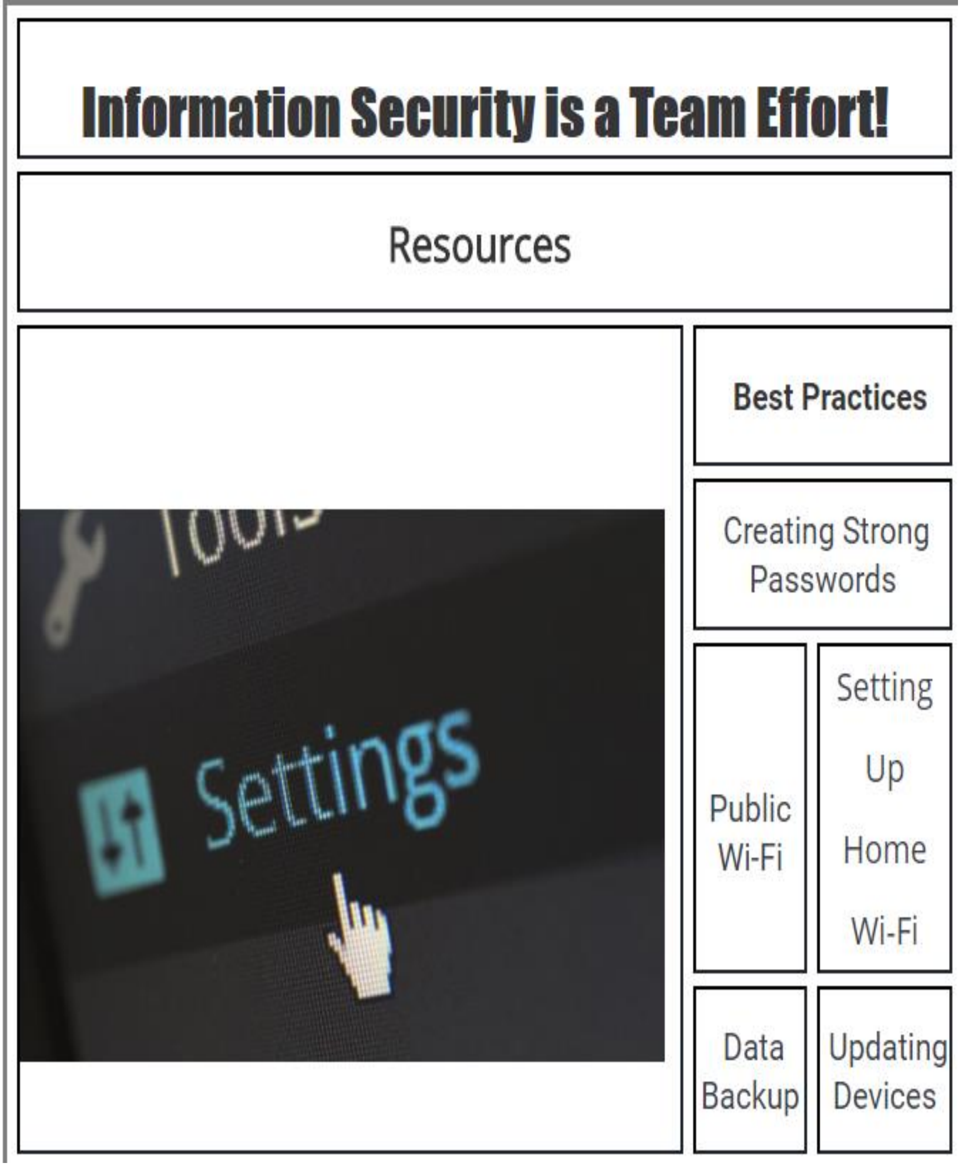
SECURE SC CITIZENS PORTAL

Resources » SecureSC

Share |

Information Security is a Team Effort!		Protect Yourself from Cyber Crime!	
Resources		Training	
	Best Practices	Texas A&M Extension Services FREE Training	
	Creating Strong Passwords		Online for Everyone – Non-Technical
	Public Wi-Fi Setting Up Home Wi-Fi		AWR 168 – Cyber Law and White Collar Crime
	Data Backup Updating Devices		AWR 174 - Cyber Ethics
	Safe Web Usage		Online for Business Professionals
	Online Shopping		AWR 169 – Cyber Incident Analysis and

SC CYBER



Information Security is a Team Effort!

Resources

Best Practices

Creating Strong Passwords

Public Wi-Fi

Setting Up Home Wi-Fi

Data Backup

Updating Devices

Safe Web Usage

Online Shopping

Social Media

Kids on the Web

Browser Security Settings

Protecting Against Cyber Threats

Phishing and Social Engineering

What is Malware?

Identity Theft

SC CYBER

South Carolina Infrastructure Protection Center

Free Online Cybersecurity Courses

SC Cyber has partnered with the Texas A&M Engineering Extension (TEEX) to provide FREE online cybersecurity courses. As a founding member of the National Domestic Preparedness Consortium (NDPC), TEEX offers a wide range of online and face-to-face cybersecurity training opportunities.

No country, industry, community or individual is immune to cyber risks. Cyber space is woven into the very fabric of our daily lives. Partnering with DHS/FEMA we are committed to ensuring cyber space is supported by secure and resilient infrastructure. Ensuring open communications, information and prosperity while protecting privacy and confidentiality.

U.S. Department of Homeland Security FEMA

Texas A&M Engineering TEEX Extension Service

SC CYBER

SC CYBER

Cybersecurity

Table Top Exercise (TTX)

Aiken County Government

Fall 2017

Scope

- This exercise is a facilitated, discussion-based exercise, planned for four hours, presented by SC Cyber.
- The exercise will raise awareness of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, and response.

Exercise Objectives

- Increase cybersecurity awareness
- Assess cybersecurity’s integration in all-hazards preparedness
- Examine cybersecurity information sharing, escalation criteria, and related courses of action
- Examine cybersecurity incident management structures
- Review cyber resource request and management processes

Core Capabilities

Protection:

- **Cybersecurity**-Protect against damage to, the unauthorized use of, and/or the exploitation of (and, if needed, the restoration of) electronic communications systems and services (and the information contained therein).

Exercise Overview

- Four-hour continuous interactive exercise

- The TTX consists of:
  - Introductions
  - Cybersecurity Awareness Briefing
  - Three Modules
  - Debrief and Evaluation

- Participant engagement encouraged

- Time awareness during questions, brief outs, etc.

Exercise Schedule

Activity	**Time**
Welcome, Introductions and Guidelines Cybersecurity Briefing	25 minutes 15 Minutes
Module 1: Preparation	60 minutes
Module 2: Detection and Analysis	60 minutes
Module 3: Containment, Eradication, and Recovery	60 minutes
Debrief and Evaluation	20 minutes

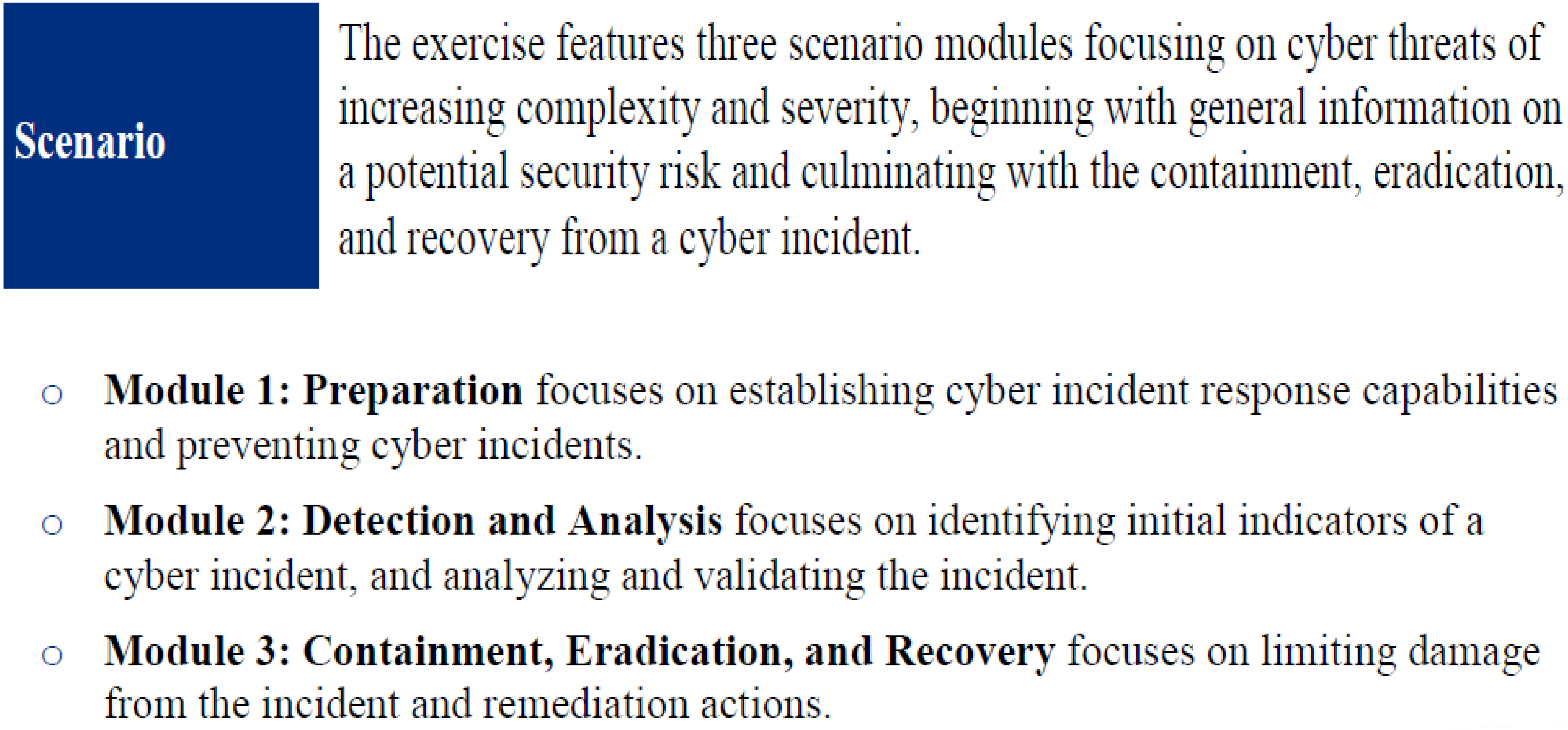
Assumption and Artificialities

- The scenario is plausible and events occur as they are presented
- There is no hidden agenda and there are no trick questions
- All players receive information at the same time

Ground Rules

- Do NOT critique the scenario
- Draw from your previous experience
- Do NOT assume information
- Participation is encouraged
- The facilitator's job is to help ***you*** come up with solutions

Scenario



Scenario

The exercise features three scenario modules focusing on cyber threats of increasing complexity and severity, beginning with general information on a potential security risk and culminating with the containment, eradication, and recovery from a cyber incident.

- **Module 1: Preparation** focuses on establishing cyber incident response capabilities and preventing cyber incidents.
- **Module 2: Detection and Analysis** focuses on identifying initial indicators of a cyber incident, and analyzing and validating the incident.
- **Module 3: Containment, Eradication, and Recovery** focuses on limiting damage from the incident and remediation actions.

Day 1 – Heads Up

- Law enforcement, IT officials, and other security staff review their respective intel and information products produced from various government and private sector sources. Information sources include, but are not limited to, Information Sharing and Analysis Center(s), Law Enforcement, the Fusion Center, and/or security vendors

- The volume of information and depth of analysis related to cyber and communications threats varies across the products

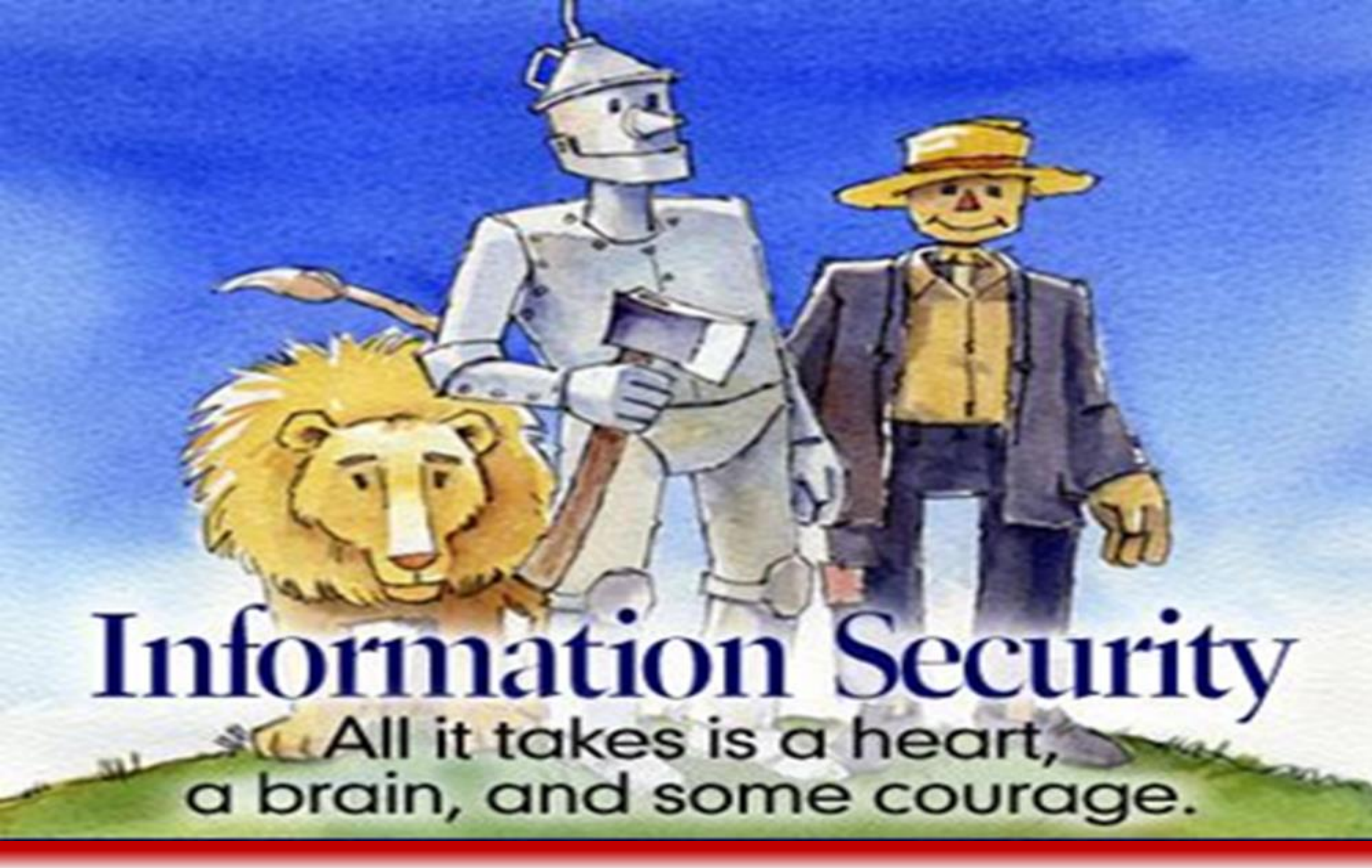
- One advisory discusses the resurgence of third party vendor exploitation. This exploitation allows attackers full access to remotely manipulate agency platforms, critical business information, personally identifiable information, and internal system processes

Module 1 – Discussion Topics

1. Internal and external sources of threat information
2. Cyber related risk assessment, planning, and capabilities
3. Essential elements of information and key questions
4. Cyber preparedness integration and awareness training
5. Cybersecurity policy integration

Day 7 – Facelift (website defacement)

- Your employees notice several cosmetic changes to your main website. They also note that a popular used link directs people to an unrelated website.


Information Security
All it takes is a heart,
a brain, and some courage.

2nd Annual Cybersecurity Summit

May 24

Francis Marion Hotel

Charleston, SC

SC CYBER

Department of Homeland Security

Cyber Capabilities/Entities

- National Cybersecurity and Communications Integration Center (NCCIC) (contact: NCCIC@hq.dhs.gov)

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (contact: ics-cert@hq.dhs.gov ; 877-776-7585)

- National Coordinating Center for Communications (NCC) (contact: NCC@hq.dhs.gov 703-235-5080)

- United States Computer Emergency Readiness Team (US-CERT) (contact: info@us-cert.gov 888-282-0870)

- National Infrastructure Coordinating Center (contact: NICC@hq.dhs.gov)

Private Sector/Business

Private Sector/Business Cyber Capabilities/Entities

- Business Executives for National Security http://www.bens.org/
- Electronic Privacy Information Center http://epic.org/

Information Sharing and Analysis Centers (ISACs)

- Internet Security Alliance http://www.isalliance.org/
- National Council of ISACs http://www.isaccouncil.org/

SCCYBER

info@sccyber.org
sccyber.org
@sc_cyber

INDUSTRY

ACADEMIA

GOVERNMENT