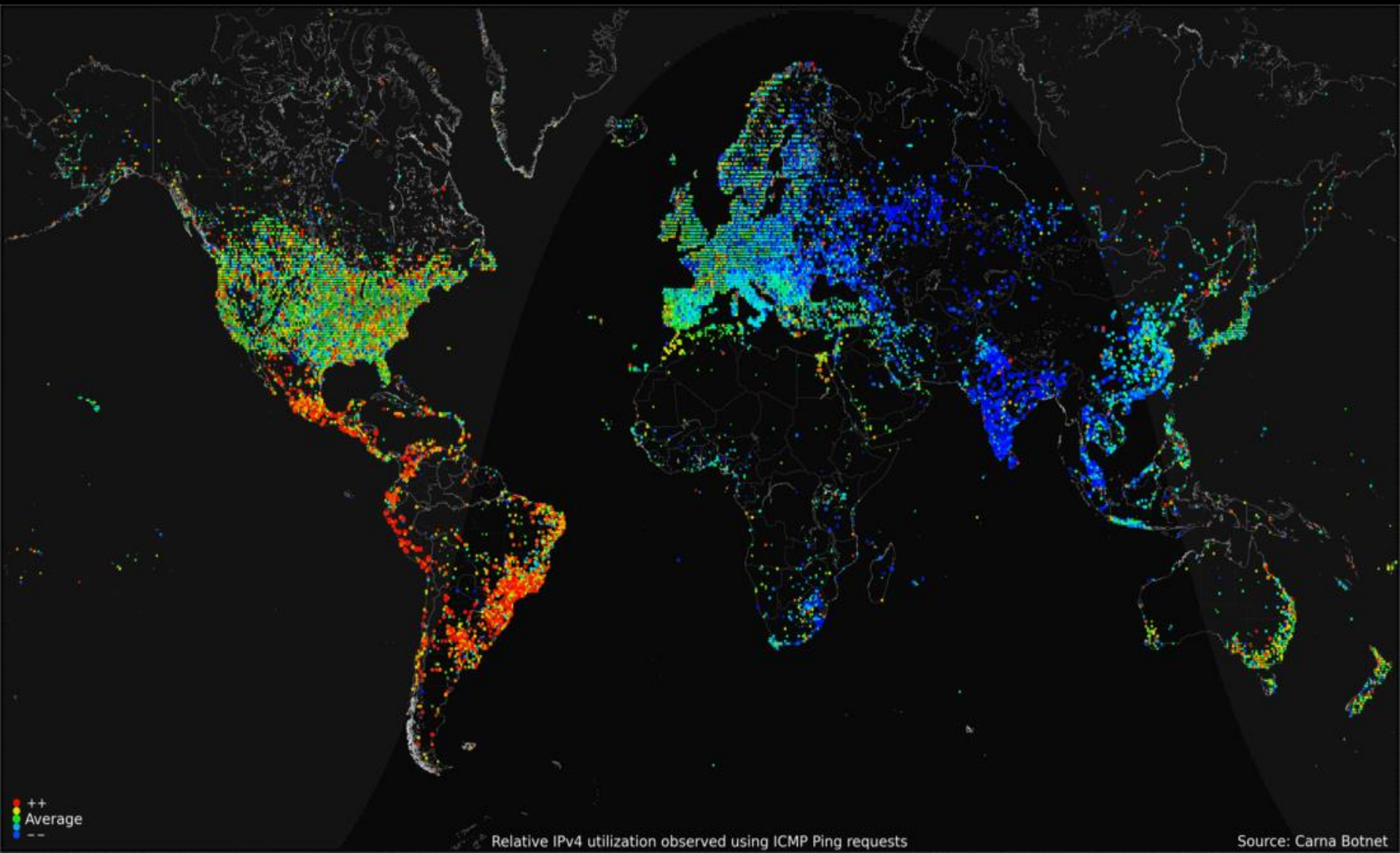
Cyber Threats, Trends, and Security Configurations

June 2, 2015

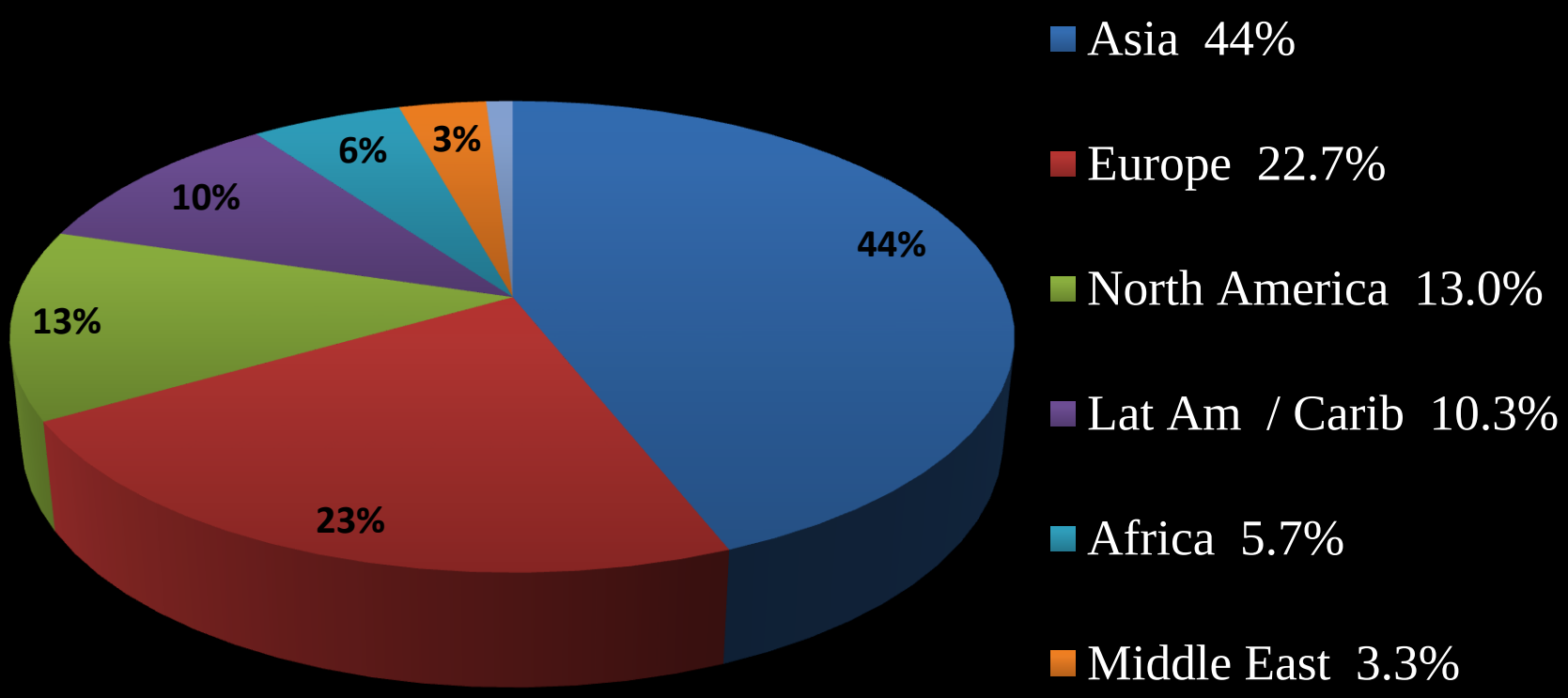
Shevaun Culmer-Reid, Program Manager

The Center for Internet Security is an international nonprofit organization focused on enhancing cyber security readiness and response for the public and private sectors.

The Internet



2.6 Billion Internet Users

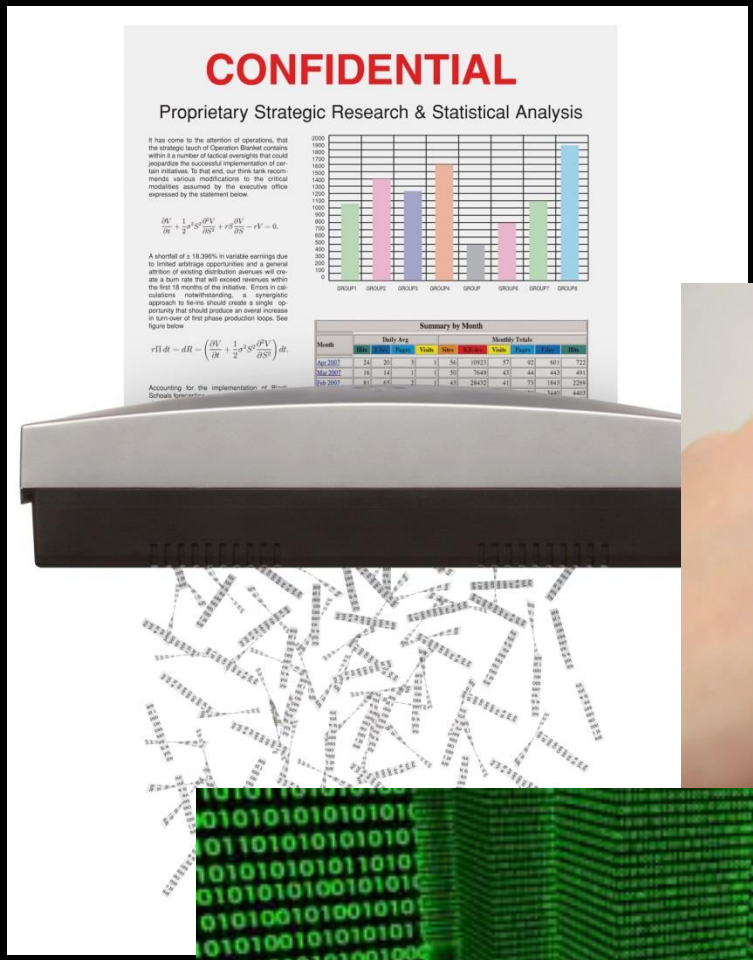


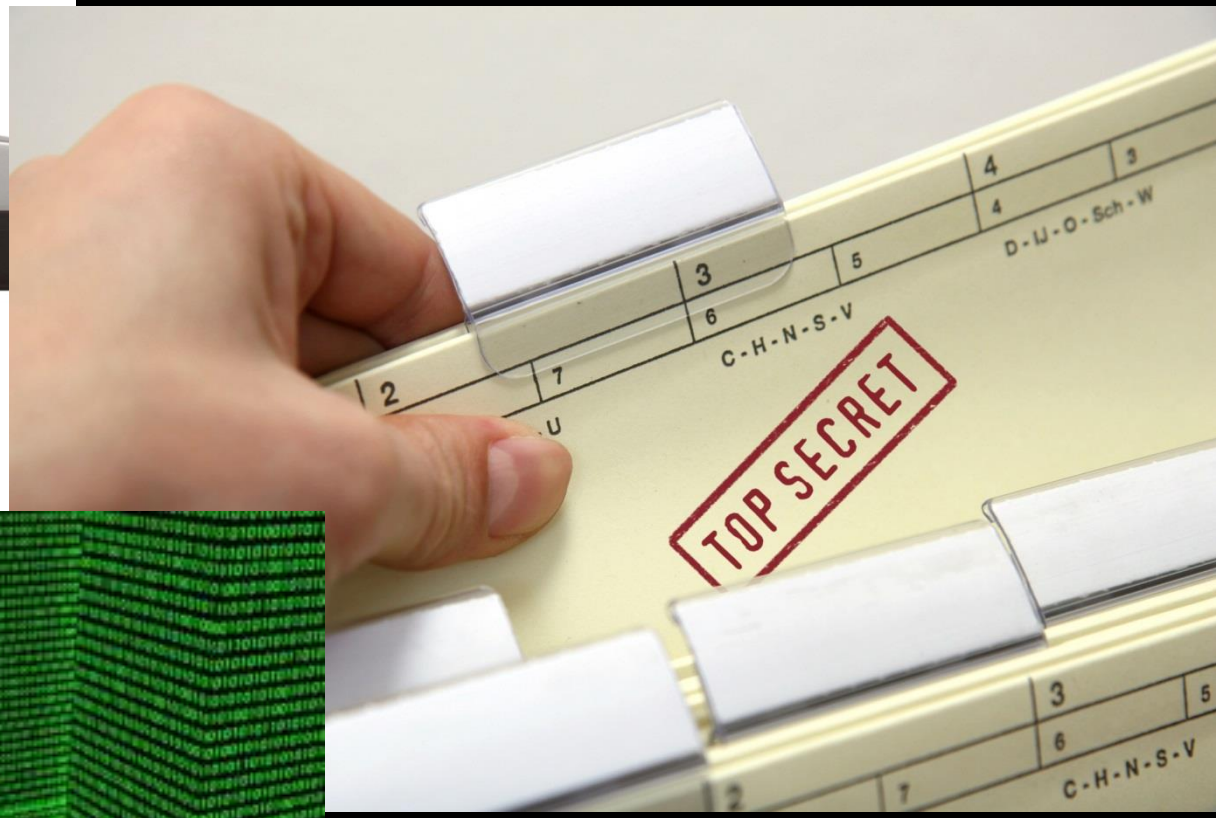
facebook

Register Now

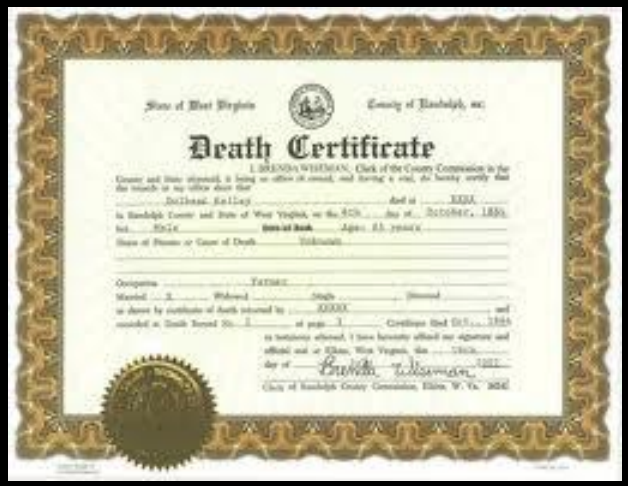
The Internet is a tremendous tool

Criminals look for data…



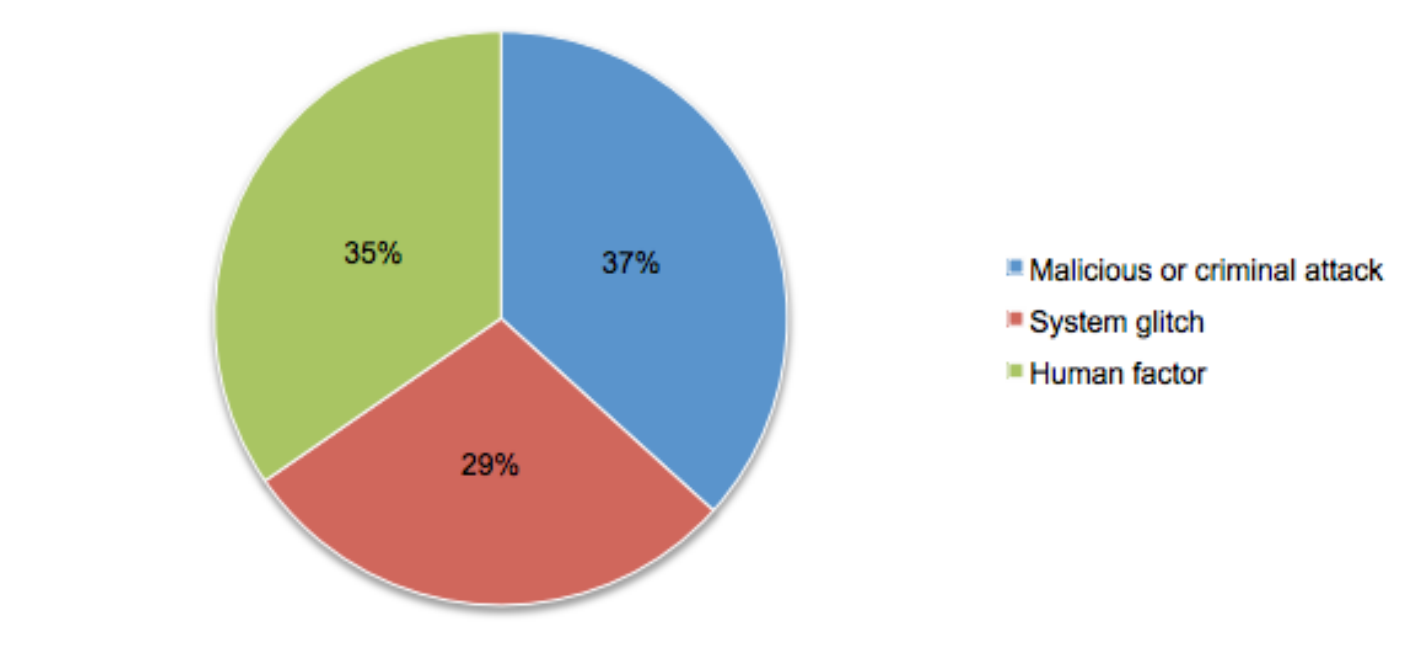


And Governments have a lot of it!



What are the causes of data breaches?

According to the Ponemon Institute, data breaches have three main causes:



By addressing vulnerabilities,
you can reduce susceptibility to these causes

Who Is Behind The Threats?

Cyber Criminals

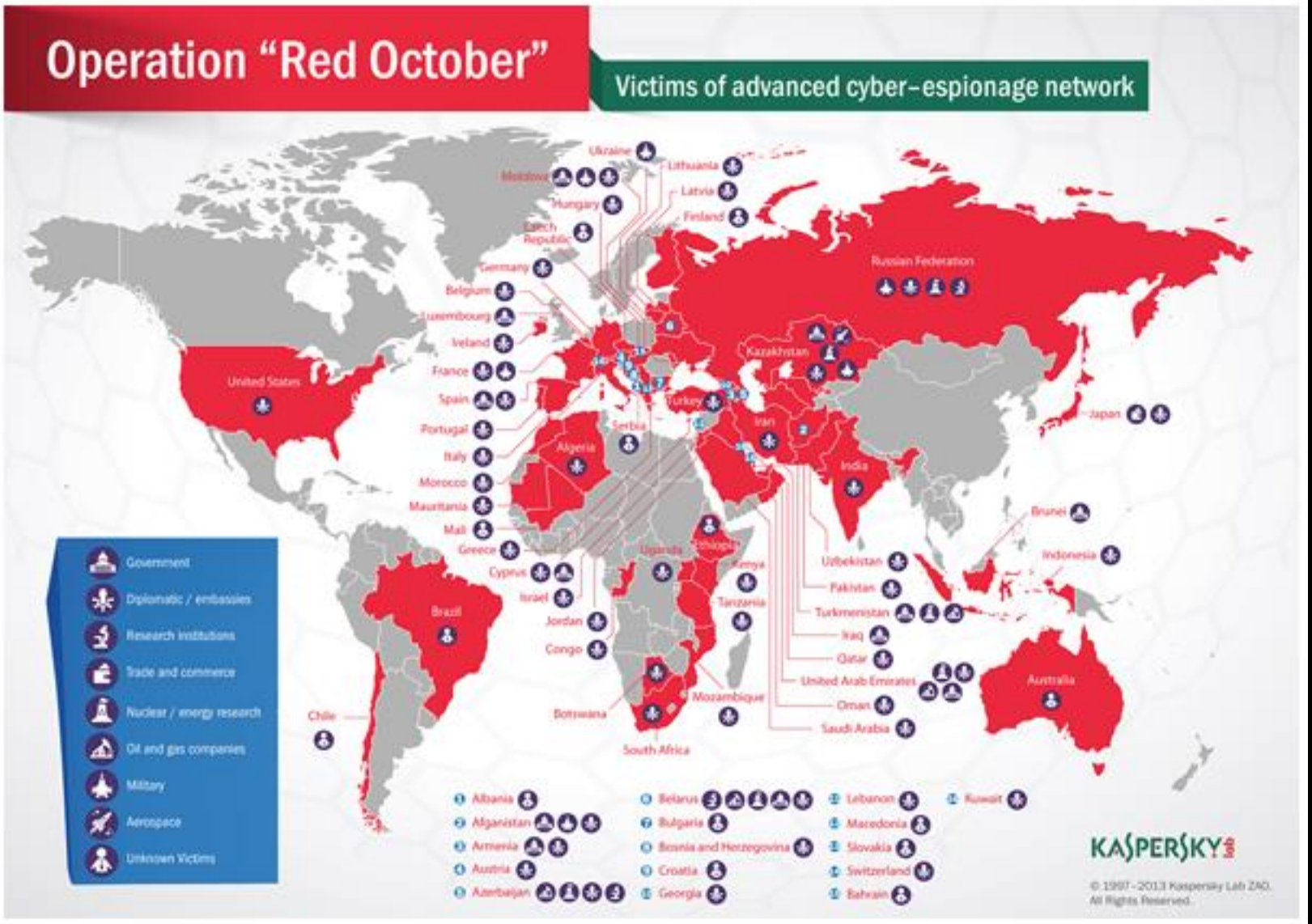
Insider Threat

Hacktivists

Nation States

Operation "Red October"

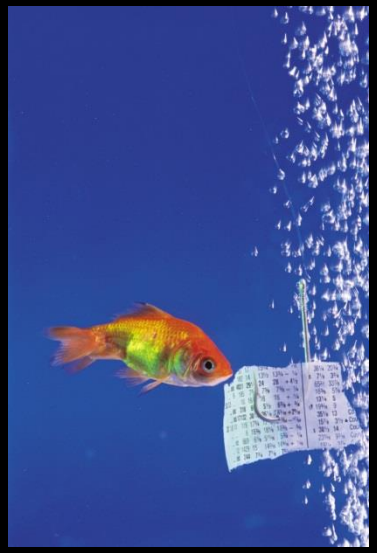
Victims of advanced cyber-espionage network



KASPERSKY

Recent Attack Trends

- Bash Bug/Shellshock
- Ransomware
- Website Defacements
- Phishing
- Denial of Service (DOS)



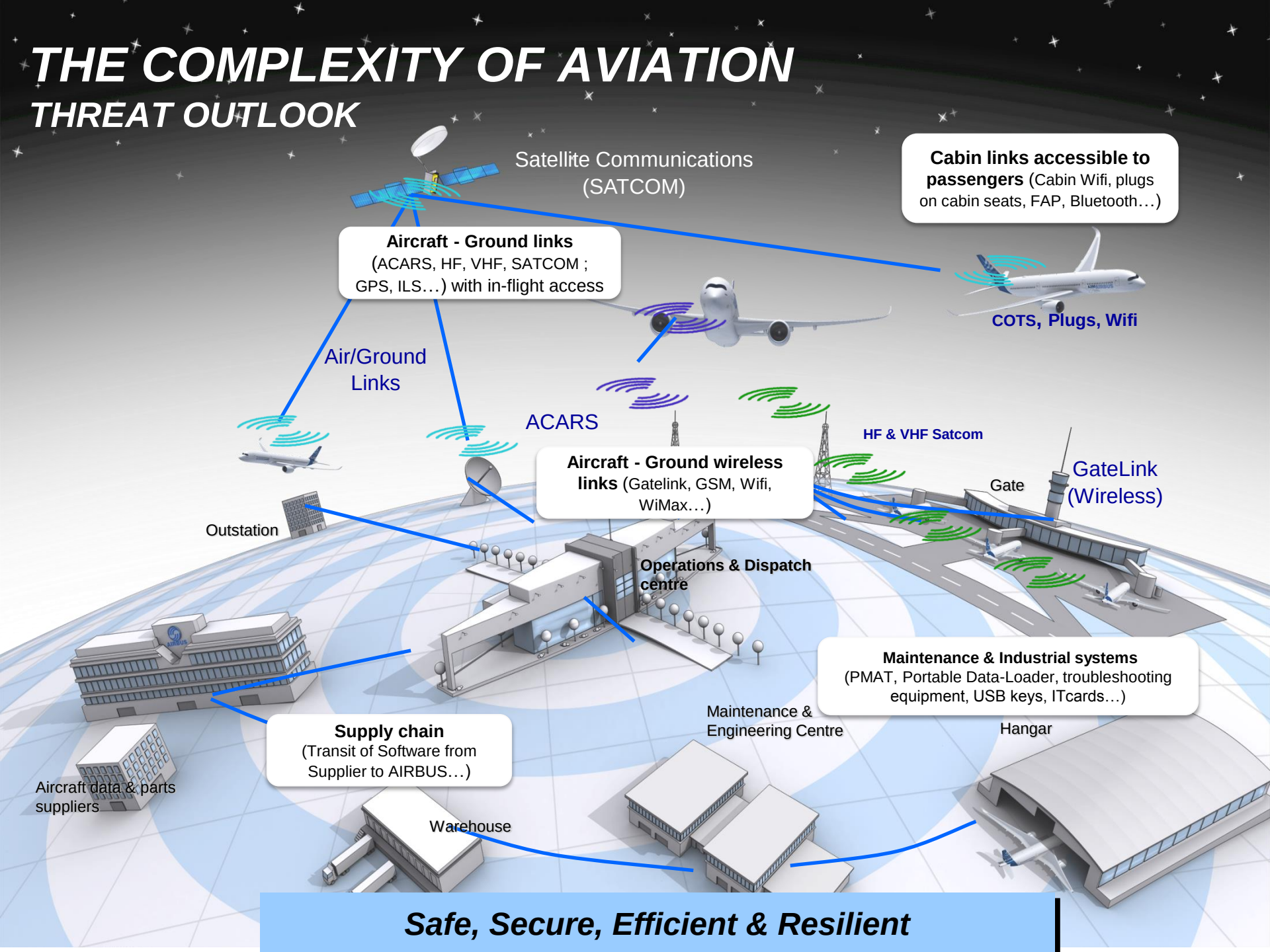
ITS

Intelligent Transportation Systems

Critical Infrastructure

THE COMPLEXITY OF AVIATION

THREAT OUTLOOK



Safe, Secure, Efficient & Resilient

Cyber Trends in Aviation

- GAO Report-Joint Intel Bulletin/PIN
  - 150420-001 Report
- Chris Roberts In-Flight Entertainment claims
- Dark Hotel Event
- Intellectual Property Theft
  - Maintenance Plans
  - Airport Design Plan
- Boarding pass and frequent flyer schemes
- Aviation ISAC Airport exercise results

Emergency Alert Systems Compromised

'Hackers' access Emergency Alert System of local Great Falls, Montana TV station to broadcast fake warning of 'Zombie Apocalypse'

Time Newsfeed
Tue, 12 Feb 2013 14:33 CST

A Montana television station's regular programming was interrupted by news of a zombie apocalypse.

The Montana Television Network says hackers broke into the Emergency Alert System of Great Falls affiliate KRTV and its CW station Monday.

KRTV says on its website the hackers broadcast that "dead bodies are rising from their graves" in several Montana counties.

The alert claimed the bodies were "attacking the living" and warned people not to "approach or apprehend these bodies as they are extremely dangerous."

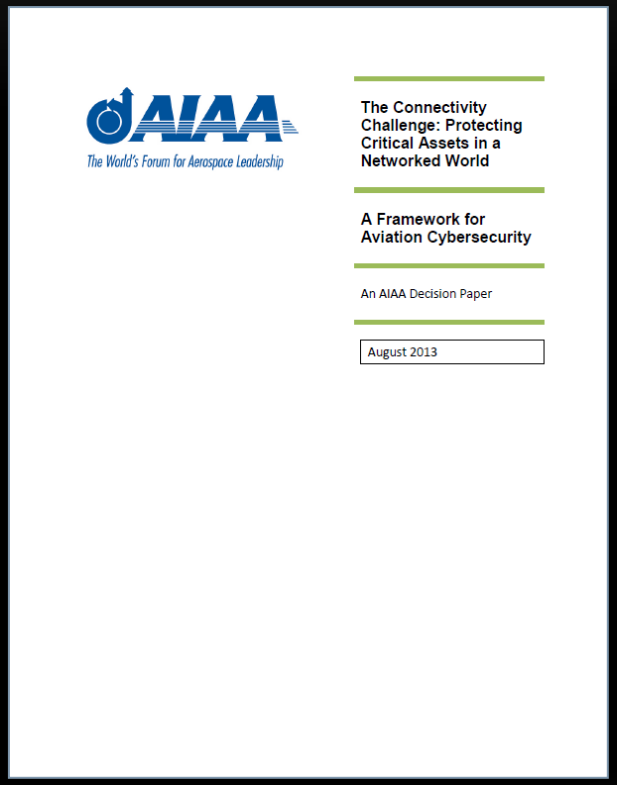
The network says there is no emergency and its engineers are investigating.

A call to KRTV was referred to a Montana Television Network executive in Bozeman. Jon Saunders didn't immediately return a call for comment.

Airport Case

- A partner notified us that several airports were targeted by an advanced hacking group
- Once we received their logs we ran them against the logs of other organizations we monitor
- 8 more groups were being impacted by these hackers
- By coordinating information between these groups a phishing email was pinpointed
- By analyzing details of the email we realized that an airport organization membership was being targeted
- We shared the information and assisted with the analysis, identifying 75 impacted airports, two with compromised systems

A FRAMEWORK FOR AVIATION CYBERSECURITY
AIAA – AUGUST 2013



Establish common cyber standards for aviation systems

Establish a cybersecurity culture

Understand the threat

Understand the risk

Communicate the threats and assure situational awareness

Provide incident response

Strengthen the defensive system

Define design principles

Define operational principles

Conduct necessary research and development

Ensure that government and industry work together

*****Yellow indicates area of A-ISAC Focus***

Resiliency Across Commercial Aviation

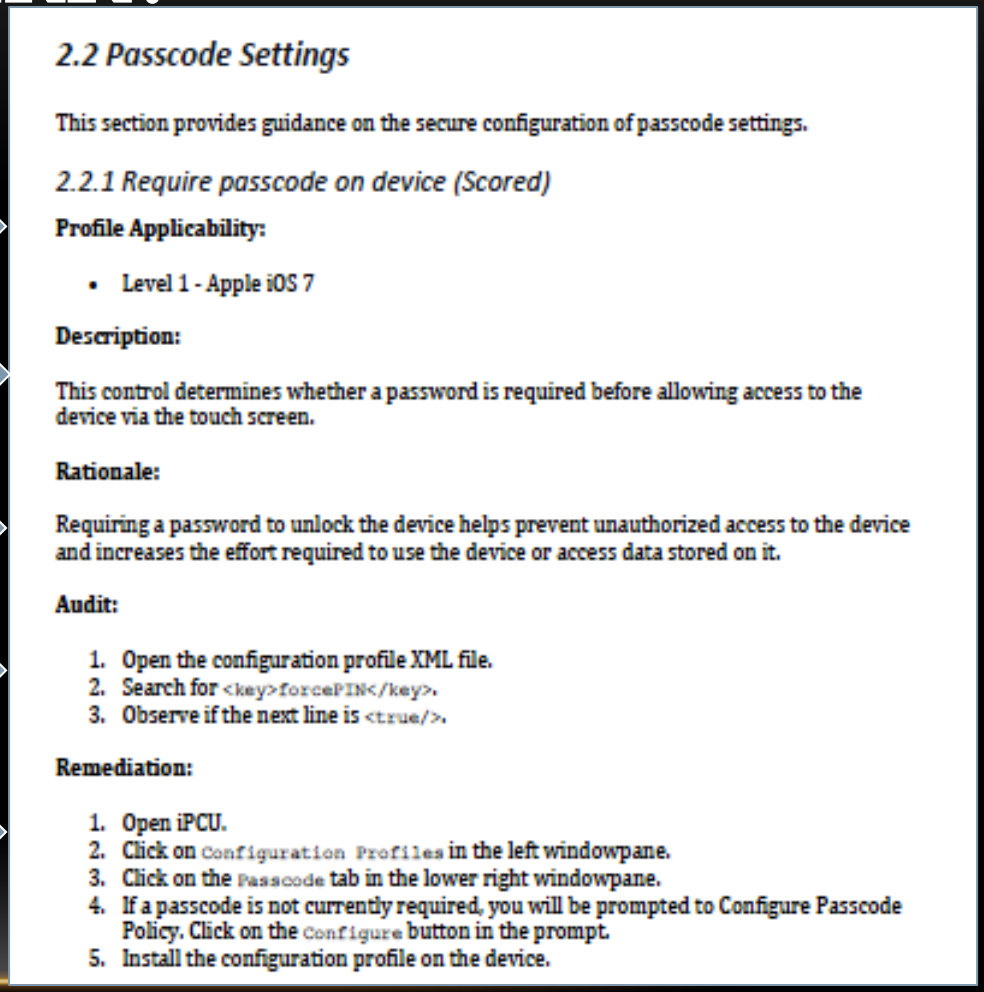
CENTER FOR INTERNET SECURITY®

Security Benchmarks™

"Measurably reducing risk through collaboration, consensus & practical security management"

WHAT IS A CIS SECURITY BENCHMARK?

- Title
- What to do…
- Why to do it…
- How to audit…
- How to fix…



2.2 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

2.2.1 Require passcode on device (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control determines whether a password is required before allowing access to the device via the touch screen.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>forcePIN</key>`.
3. Observe if the next line is `<true/>`.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. If a passcode is not currently required, you will be prompted to Configure Passcode Policy. Click on the `Configure` button in the prompt.
5. Install the configuration profile on the device.

HOW ARE CIS BENCHMARKS DEVELOPED?

- International Consensus Process
- Join a Consensus Team
  - Log in to the member community site: https://community.cisecurity.org
- Participants
  - Review Draft
  - Review and respond to discussions
  - Test Configurations
  - Report Bugs/Suggestions

CONFIGURATION CONTENT: PORTFOLIO

- **Authentication Servers**
  - FreeRADIUS 1.1.3
  - MIT Kerberos 1.0
- **Collaboration Servers**
  - Microsoft SharePoint Server 2007
- **Database Platforms**
  - IBM DB2 Server 8/9/9.5
  - Microsoft SQL Server 2000/2005/2008 R2/2012/2014
  - MySQL Database Server 4.1/5.0/5.1/5.6
  - Oracle Database Server 8i/9i/10g/11g R2
  - Sybase Database Server 15
- **Directory Servers**
  - Novell eDirectory 8.7
  - OpenLDAP Server 2.3.39/2.4.6
- **DNS Servers**
  - BIND DNS Server 9.0-9.5
- **Mail Servers**
  - Microsoft Exchange 2003/2007/2010/2013
- **Mobile Platforms**
  - Apple Mobile Platform iOS 5/6/7
  - Google Mobile Platform
- **Network Devices**
  - Checkpoint Firewall
  - Cisco Firewall Devices
  - Cisco Routers/Switches IOS 12.x
  - Cisco Wireless LAN Controller 7
  - Juniper Routers/Switches JunOS 8/9/10
  - Agnostic Print Devices
- **Productivity Software**
  - Microsoft Office 2007
  - Microsoft Outlook 2010
- **Operating Systems - Desktop**
  - Apple Desktop OSX 10.4/10.5/10.6/10.8/10.9/10.0
  - Microsoft Windows Desktop XP/NT/7/8.1
- **Virtualization Platforms**
  - VMware Server 3.5/4.1/5.1/5.5, 5.5 Update 2
  - Xen Server 3.2
  - Agnostic VM Server
- **Operating Systems - Servers**
  - CentOS 6 / 7
  - Debian Linux Server
  - FreeBSD Server 4.1.0
  - HP-UX Server 11iv2/3 Update 4
  - IBM AIX Server 4.3.2/4.3.3/5L/5.1/5.3/6.1/7.1
  - Microsoft Windows Server 2000 Pro/2003 DC & MS/2008 DC & MS/2008 R2 DC & MS/ 2012 R2 DC & MS/ 2012 DC & MS
  - Novell Netware
  - Oracle Solaris Server 2.5.1-11.1/ 10 updates 3-8
  - Red Hat Linux Server 4/5/6/7
  - Slackware Linux Server 10.2
  - SUSE Linux Enterprise Server 9/10/11
  - Ubuntu LTS Server 12.04/14.04
  - Amazon Linux 2014.09
  - Oracle Linux 7
- **Web Browsers**
  - Apple Safari Browser 4.x
  - Microsoft Internet Explorer 9/10
  - Mozilla Firefox Browser 3.6/24 ESR
  - Opera Browser 10
- **Web Servers**
  - Apache HTTP Server 2.2/2.4
  - Apache Tomcat Server 5.5/6.0
  - Microsoft IIS Server 5/6/7/7.5/8

WHY IS IT IMPORTANT TO HAVE SECURE CONFIGURATIONS?

Risks of not having secure configurations

- Leaving systems vulnerable to exploitation
- Susceptible to Data breaches
- Possible Loss of Control of systems

HP Cyber Risk Report (2015)

- **Highlights and key findings**
- **44 percent of known breaches came from vulnerabilities that are 2-4 years old.** Attackers continue to leverage well-known techniques to successfully compromise systems and networks. Every one of the top ten vulnerabilities exploited in 2014 took advantage of code written years or even decades ago.
- **Server misconfigurations were the number one vulnerability.** Over and above vulnerabilities such as privacy and cookie security issues, server misconfigurations dominated the list of security concerns in 2014, providing adversaries unnecessary access to files that leave an organization susceptible to an attack.

WHAT IS CIS-CAT?

- A Configuration assessment tool
- Assesses a target system against recommendations made in CIS 50+ Security Benchmarks
- Benchmark policy can be customized within the tool
- Run on multiple systems at one time, set-up to run on scheduled task
- Vulnerability Assessment (MS Windows XP, 7, 8, 8.1, Server 2008, 2008 R2, Server 2012, Server 2012 R2 and RHEL 4 & 5)
- Security Content Automation Protocol (SCAP) 1.2 Validation as an Authenticated Configuration Scanner from National Institute of Standards and Technology (NIST)
- Available to CIS Security Benchmarks members only

WHY WOULD YOUR ORGANIZATION USE IT?

- Server admins/operations teams use CIS-CAT to perform self assessments.
- IT teams use CIS-CAT to validate a system before new platform upgrades.
- Security teams use CIS-CAT as part of their assessment process.
- Auditors use CIS-CAT as part of compliance and governance processes.
- Organizations don’t have to spend time developing security standards, and can rapidly assess against them.
- Users receive free technical support.

ASSESS A TARGET SYSTEM…

Select a CIS Benchmark

From the drop-down

Report Summary

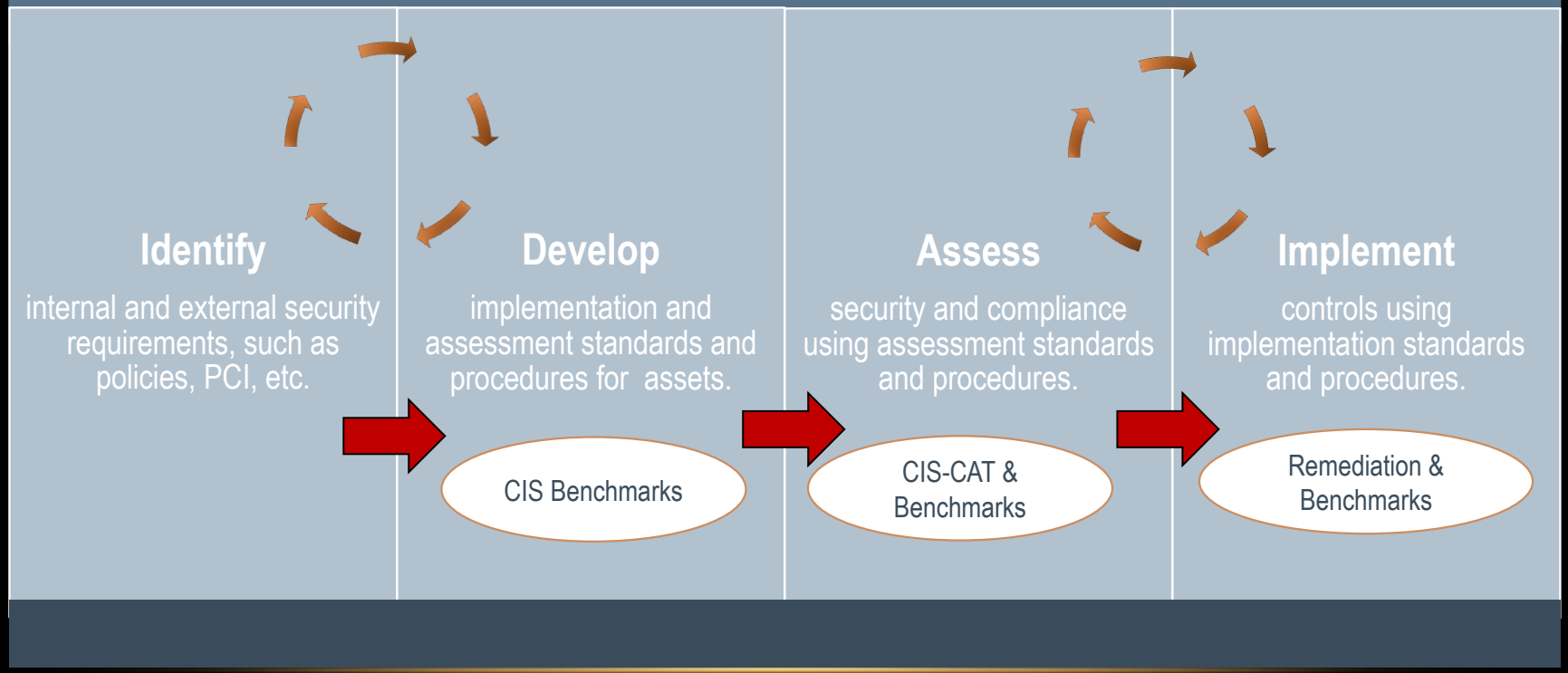
Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Computer Configuration	**202**	**2**	**0**	**3**	**202.0**	**207.0**	**98%**
1.1 Administrative Templates	35	0	0	0	35.0	35.0	100%
1.1.1 Windows Components	19	0	0	0	19.0	19.0	100%
1.1.1.1 BitLocker Drive Encryption	0	0	0	0	0.0	0.0	0%
1.1.1.1.1 Operating System Drives	0	0	0	0	0.0	0.0	0%
1.1.1.1.2 Fixed Data Drives	0	0	0	0	0.0	0.0	0%
1.1.1.1.3 Removable Data Drives	0	0	0	0	0.0	0.0	0%
1.1.1.2 AutoPlay Policies	1	0	0	0	1.0	1.0	100%
1.1.1.3 Event Log Service	6	0	0	0	6.0	6.0	100%
1.1.1.3.1 Application	2	0	0	0	2.0	2.0	100%
1.1.1.3.2 Security	2	0	0	0	2.0	2.0	100%
1.1.1.3.3 System	2	0	0	0	2.0	2.0	100%
1.1.1.4 Windows Remote Shell	1	0	0	0	1.0	1.0	100%
1.1.1.5 Windows Explorer	1	0	0	0	1.0	1.0	100%
1.1.1.6 Windows Update	5	0	0	0	5.0	5.0	100%
1.1.1.7 Credential User Interface	1	0	0	0	1.0	1.0	100%
1.1.1.8 Remote Desktop Services	4	0	0	0	4.0	4.0	100%
1.1.1.8.1 Remote Desktop Session Host	3	0	0	0	3.0	3.0	100%
1.1.1.8.1.1 Security	2	0	0	0	2.0	2.0	100%
1.1.1.8.1.2 Device and Resource Redirection	1	0	0	0	1.0	1.0	100%
1.1.1.8.2 Remote Desktop Connection Client	1	0	0	0	1.0	1.0	100%
1.1.1.9 HomeGroup	0	0	0	0	0.0	0.0	0%
1.1.2 System	16	0	0	0	16.0	16.0	100%
1.1.2.1 Power Management	2	0	0	0	2.0	2.0	100%
1.1.2.1.1 Sleep Settings	2	0	0	0	2.0	2.0	100%
1.1.2.2 Internet Communication Management	7	0	0	0	7.0	7.0	100%
1.1.2.2.1 Internet Communication settings	7	0	0	0	7.0	7.0	100%
1.1.2.3 Remote Procedure Call	2	0	0	0	2.0	2.0	100%
1.1.2.4 Remote Assistance	2	0	0	0	2.0	2.0	100%
1.1.2.5 Group Policy	3	0	0	0	3.0	3.0	100%
1.1.2.6 Logon	0	0	0	0	0.0	0.0	0%
1.2 Windows Settings	167	2	0	3	167.0	172.0	97%
1.2.1 Security Settings	167	2	0	3	167.0	172.0	97%
1.2.1.1 Local Policies	86	2	0	1	86.0	89.0	97%
1.2.1.1.1 Security Options	56	2	0	1	56.0	59.0	95%
1.2.1.1.2 User Rights Assignment	30	0	0	0	30.0	30.0	100%
1.2.1.2 Advanced Audit Policy Configuration	53	0	0	0	53.0	53.0	100%

Monitor Progress

FREE “45-day” CIS-CAT trial available
*Mention this meeting for the extended trial

Common Workflow used by CIS Members



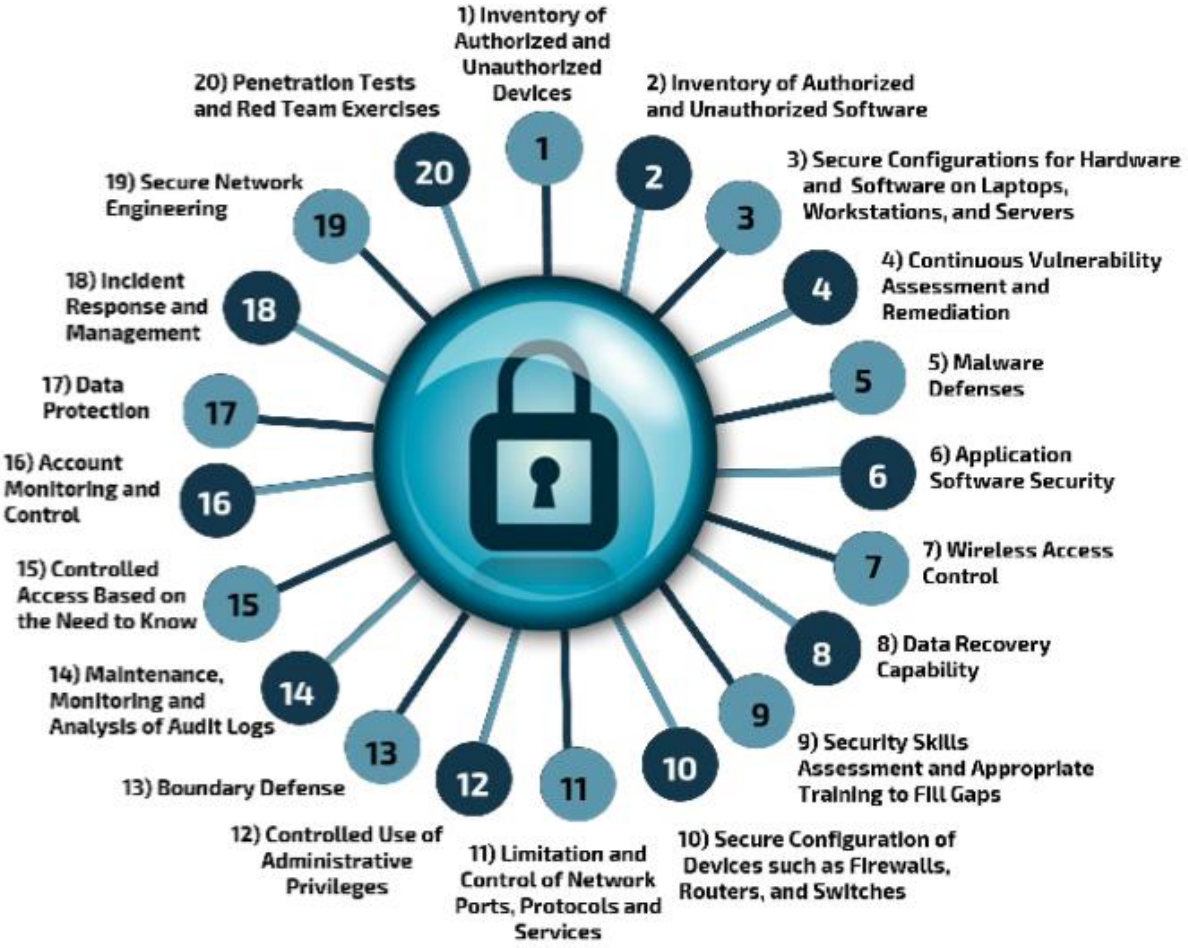
What can you do?

Leadership, Governance, Responsibility (Assign), Compliance (Measure)

- Securely configure systems
- Keep your systems patched
- Update cyber security policies
- Monitor compliance with the policies
- Regularly scan systems
- Backup your systems on a regular basis and store off site
- Encrypt your mobile devices
- Train your users

Critical Security Controls

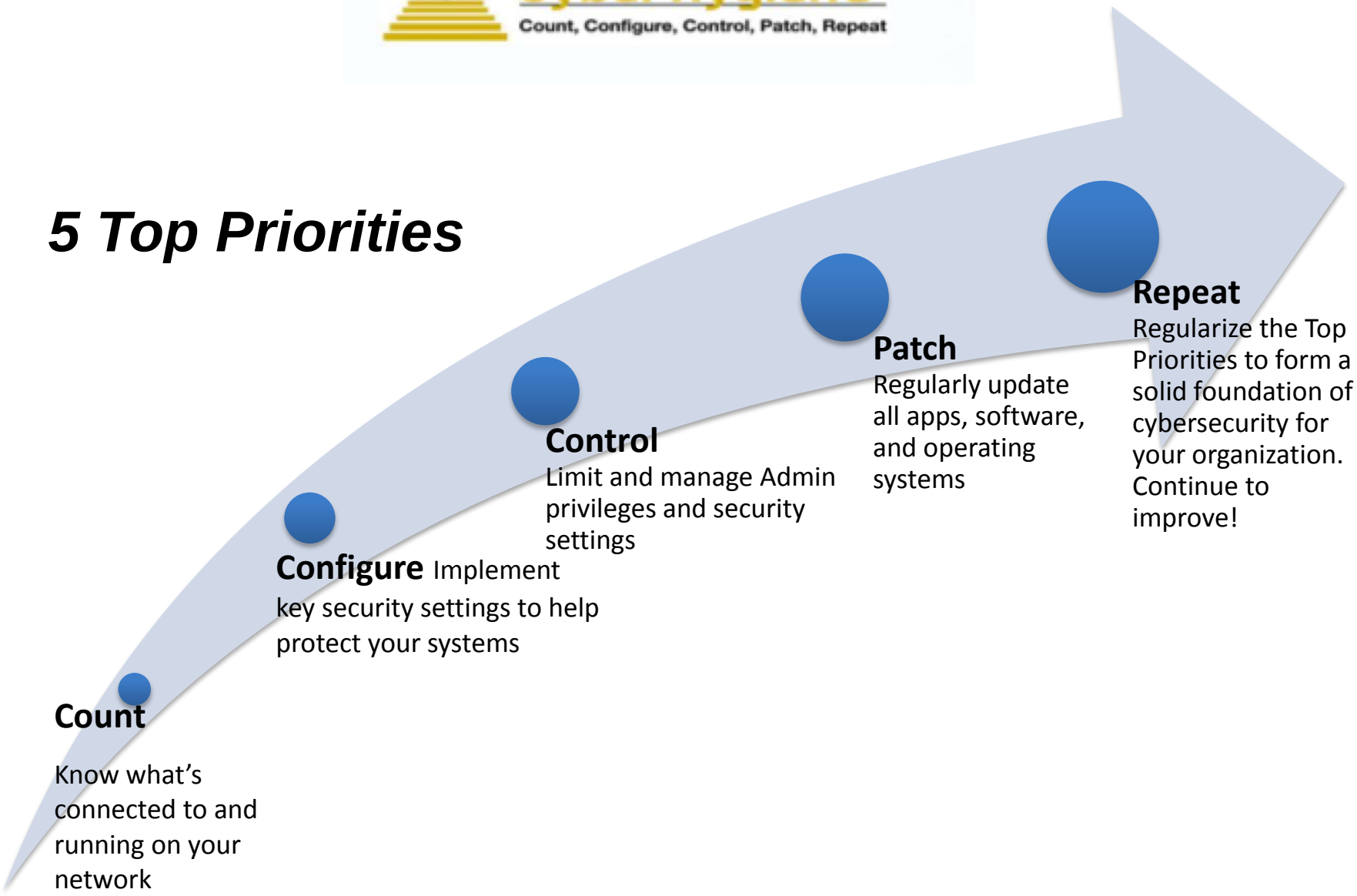
Specific and actionable ways to thwart today's most pervasive attacks



National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

5 Top Priorities



Count

Know what's connected to and running on your network

Configure Implement key security settings to help protect your systems

Control

Limit and manage Admin privileges and security settings

Patch

Regularly update all apps, software, and operating systems

Repeat

Regularize the Top Priorities to form a solid foundation of cybersecurity for your organization. Continue to improve!

Resources

- **CIS Resources**
  - Daily cyber tips
  - Over 100 Security Benchmarks via Free PDF
  - Free 45-day CIS-CAT trial – mention this meeting for extended trial
  - Monthly newsletters
  - Webcasts
  - Guides
  - Security Benchmarks Paid Membership
- **Aviation ISAC Resources**
  - Free daily aviation related cyber memos
  - Aviation ISAC Paid Membership

How does sharing information help protect your organization from attackers?

- Be prepared
  - Learning from others' best practices makes your organization stronger
  - Gather intelligence to help you be proactive
- Be willing to ask for help
  - Identify other resources to augment what you are doing
- Be a part of the solution
  - Take part in information sharing

Contact Information

Center for Internet Security

Shevaun Culmer-Reid
Program Manager
Shevaun.culmer-reid@cisecurity.org
518-880-0741

Aviation Information Sharing & Analysis Center (A-ISAC)

Faye Francy
Executive Director
Faye.i.francy@boeing.com
703-861-5417