DATA COMPLIANCE & CYBER SECURITY

PROTECT YOUR DATA. ASSESS YOUR RISK.

Berry·Talbot·Royer
CERTIFIED PUBLIC ACCOUNTANTS

SOPHOS

BizCompass
Maines Technology Leader in Managed Services
InformationTechnology CloudHosting DataProtection

---

m3ip, Inc.
Managing Your Security And Risk Needs

PATCO Construction, Inc.

Introductions

Michael Royer: Michael is the president and managing partner of Berry Talbot Royer. He has over 25 years of accounting experience working at the international accounting firm Arthur Anderson and Co., a "Big 8" accounting firm, as well as at Reliant Energy, a Fortune 500 company, based in Houston Texas. Currently, he is in charge of the corporate and individual tax and accounting team at Berry Talbot Royer. Michael is a member of the American Institute of Certified Public Accountants, the Maine Society of Certified Public Accountants, and the National Society of Tax Professionals.

Marc R. Roy: Marc has been a part of the BTR team since 2014. He earned his master's degree in Accounting and Financial Management in 2010 from the University of Maryland University College, and has been in public accounting since then. Before changing careers into accounting, Marc was a signals analyst with U.S. Navy and with the defense contractor Northrop Grumman Corporation. He is a Certified Public Accountant and a member of the American Institute of Certified Public Accountants and the Maine Society of Certified Public Accountants.

Mark Turner: Mark Turner is a senior channel account executive at Sophos covering the New England region. With over 10 years of industry experience in areas such as data protection, web security, email security and network security. Mark manages and consults with customers and partners on their security architecture and data protection strategies. Marks goal is to educate and guide organizations to a better security policy that is robust and simple to manage.

Introductions

John Burghardt: With higher education in Canada and Maine, John Burghardt is certified in many IT engineering solutions. John has been designing and planning business technology strategies for close to 20 years. While working for some of Southern Maine's IT companies, John's desire to own his own business grew, all while continuing to pioneer new solutions. John ventured into small business ownership and formed The BC Group, along with 2 other successful businesses. BC Group, was one of the first businesses in Maine to offer Disk to Disk (D2D) based backup solutions. D2D was breaking the industry standard of tape backup and delivering fast enterprise-grade backups and recovery.

Michael Desrosiers: Michael has 33+ years in the Information Technology and Security industry and has been with m3ip, Inc. for 13 years. He has worked on numerous security projects with m3ip and IBM across many enterprise security products and was Lead Principal on several large-scale implementations and delivery of numerous penetration tests and security auditing engagements. Michael is well versed in industry standards and best practices, including the ISO 27002:2013 and BS7799 security standards, COBiT, NIST and Gramm-Leach-Bliley from both policy development and compliance auditing perspectives.

Mark Patterson: Our special guest speaker! A Sanford native, Mark graduated from UMO with a degree in Business Administration / Marketing. Mark started PATCO with his Father in 1985. Always on the go, he enjoys volleyball, boating, snowboarding, waterskiing, and family time. Creating comfortable homes - within budget - for Maine families brings him the greatest satisfaction. In 2009, PATCO was an unfortunate victim of ACH Fraud (Automated Clearing House Fraud) and will be sharing his story with us. Not only has Mark been through it himself, but he has helped others to understand the risks, how to prevent such disaster and what to do when it does happen.

An ACH Fraud Story

A GLIMPSE OF WHEN IT HAPPENED, HOW IT HAPPENED, & WHAT HAPPENED NEXT.

Cyber Security {Red Flags}

. . . as told by a general contractor and small business owner.

- Sometime prior to our ACH fraud incident, we logged into our account, inserted our passwords/security questions and the screen was wrong and static. We called the local branch and were told to try again……flag
- Traces of the Zeus Trojan/malware were found on one of our accounting department's computers after the fraud……..flag.
- We used ACH transfers to transfer deposits from Chittenden/People's United Bank to another and to perform automatic payroll deposits for our employees as a convenience to them. It was a major approval process with the bank to allow this……flag
- I received a letter via US Mail from the bank on Wednesday, May 13, 2009 stating that one of our ACH transfers requested on the previous Thursday, May 7, 2009 was not completed due to an invalid receiving account in California…….flag.
- **We had requested email notifications of these transfers, but it was never implemented.**
- I assumed it was an error message because we had no employees in California and the amount was extremely high. We called the bank on the morning of Thursday, May 14, 2009.
- The bank did not know that anything was wrong……flag

PATCO CONSTRUCTION, INC.
patco.com

- The bank discovered that over the course of five nights, the following money was transferred from our account:

Thursday, May 7, 2009	$56,594.
Monday, May 11, 2009	$115,620
Monday, May 12, 2009	$99,068
Tuesday, May 13, 2009	$91,959
Wednesday, May 14, 2009	$113,647

  The transfers were initiated from an IP address never used by us and went to individual bank accounts we have never transferred to before. The banks monitoring software was posting notices that these were highly unusual transfers, initiated from IP addresses in Eastern Europe and highly suspicious…….flag……..**No one at the bank was reviewing the reports that would have notified them of this.**

Thursday, May 14, 2009	$111,963

  Even though we had notified the bank at 11:45 am that morning, the bank did not review outgoing batches in progress from the previous night and the money above was transferred from our account.

- **A total of over $588,000 was transferred out of our bank account -- without our consent.**
- People's United was able to block or recover $243,406 of the transfers. Our net loss was **$345,000.**
- The bank stated they were not responsible and it was our problem. We attempted to negotiate a settlement with our bank. We sued the bank to recover our losses, the interest we were being charged on our line of credit and our legal fees.
- We lost at the Federal District Court in Portland. We appealed at the First District Court of appeals in Boston. The banks security measures were found unreasonable and the case was remanded back to the Portland court to determine if our security measures were reasonable. We settled for the original loss amount plus interest in the fall of 2011. Legal fees are not obtainable in this type of commercial lawsuit. Our legal fees were well into the 6 figures. We were told the banks legal fees were in the 7's.

Even if your money is in the bank, it is not safe from theft in this electronic world.

PATCO CONSTRUCTION, INC.
patco.com

10 {+1} Ways to Avoid Being a Victim

. . . as told by a general contractor and small business owner.

1. Sign your own checks and review the back up (i.e. approved invoices, etc.) NO STAMPS!
2. Have all bank statements emailed or mailed to your home. Personally open the envelope and review each check copy. Look for strange recipients or unusual amounts.
3. Avoid ACH transactions. THEY ARE NOT SAFE!
4. If you must do ACH transactions, review your agreement with your bank. Know your responsibilities. IT'S SCARY!
5. Practice out of band verification. Personally call someone you know at the bank to authorize the transaction.
6. Check your bank account online every day. ACH transfers are gone for good in 24 hours.
7. Obtain cyber theft/fraud insurance. A standard commercial policy has a limit of $10,000. Your business accounts are not protected from fraud by Regulation E (protects consumers only). FDIC insurance is not applicable.
8. Do not tie savings accounts or lines of credit to checking accounts with ACH capability for over draft protection.
9. Educate your employees on safe internet browsing and email practices. When in doubt, do not click on it.
10. Install and keep a quality firewall and anti-virus software updated.
11. Trust and verify. Whether it be your employees, your children or the country of Iran, it is always good practice. If one knows you are watching, it curbs abuse.

PATCO CONSTRUCTION, INC.
patco.com

…In's & Outs of Cybersecurity

Michael Desrosiers
Principal
m3ip, Inc.

Agenda

- Introduction
- What is Cybersecurity?
- The Cybersecurity Puzzle
  - Identify, Manage & Protect
- Cyber Security Testing
  - Things That Go Bump In The Night
- Cybersecurity Review

m3ip, Inc.
Managing Your Security And Risk Needs

Introduction

- Who am I?
- What is m3ip?
- This presentation is meant to be informal and very flexible.

m3ip, Inc.
Managing Your Security And Risk Needs

There is no security on this earth; there is only opportunity.”

General Douglas MacArthur

m3ip, Inc.
Managing Your Security And Risk Needs

What is Cybersecurity?

- cybersecurity
  - /sībərsiˈkyo͝orədē/
    - noun: **cybersecurity**
- the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Google Search - 2015

m3ip, Inc.
Managing Your Security And Risk Needs

2015 Computer Crime & Security Survey Highlights

Respondents detected a wide range of attacks and abuses:

- **Forty percent** detected system penetration from unauthorized locations.
- **Seventy-eight percent** detected employee abuse of Internet access privileges (for example, downloading inappropriate material or pirated software, or inappropriate use of e-mail systems).
- **Eighty-five percent** detected computer viruses or malware.

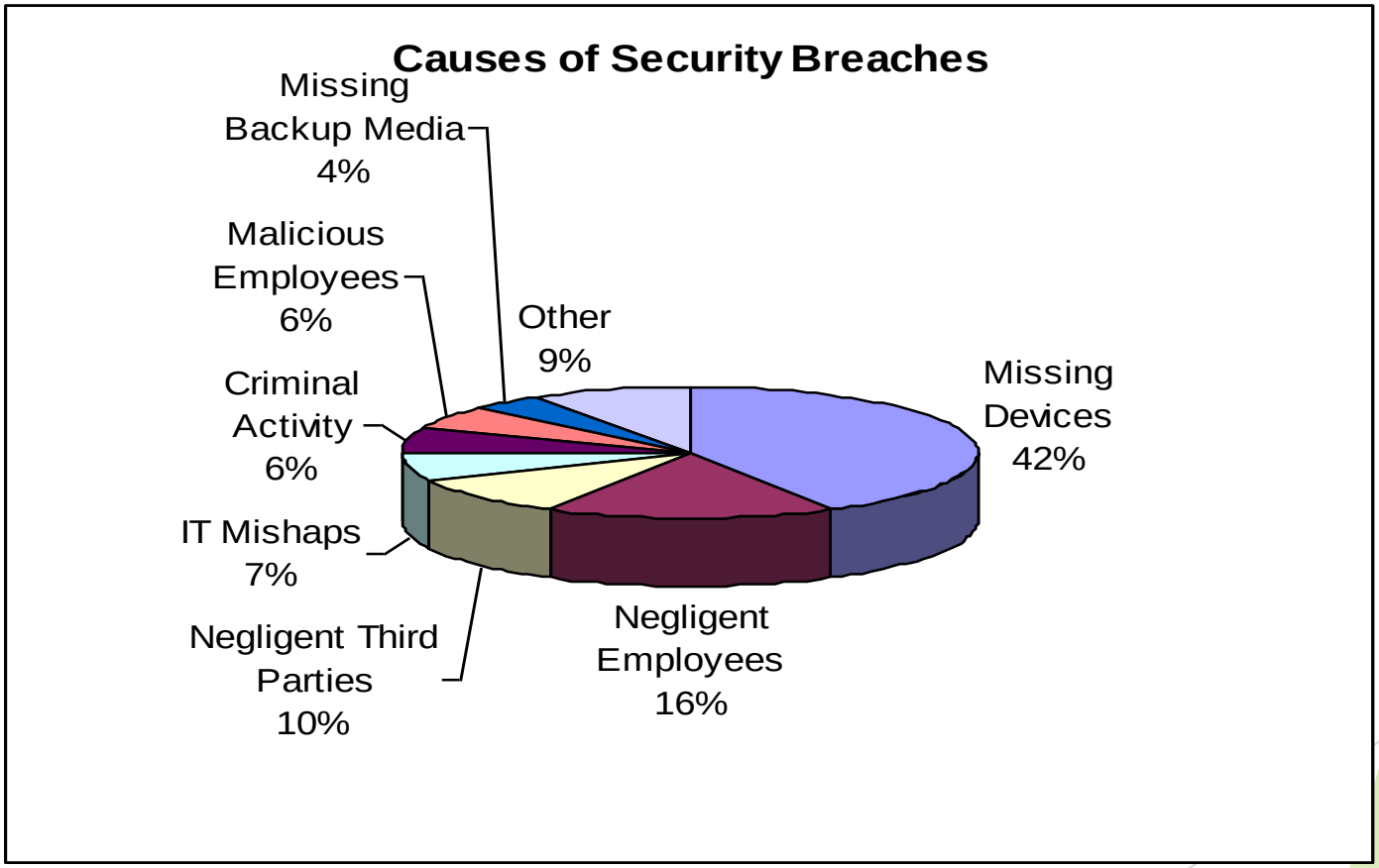
m3ip, Inc.
Managing Your Security And Risk Needs

SANS Institute Facts

- The majority of the successful attacks on operating systems come from only a few software vulnerabilities.
- This can be attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools.
- They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems.

m3ip, Inc.
Managing Your Security And Risk Needs

2014 Ponemon Institute National Study of Data Loss Breaches

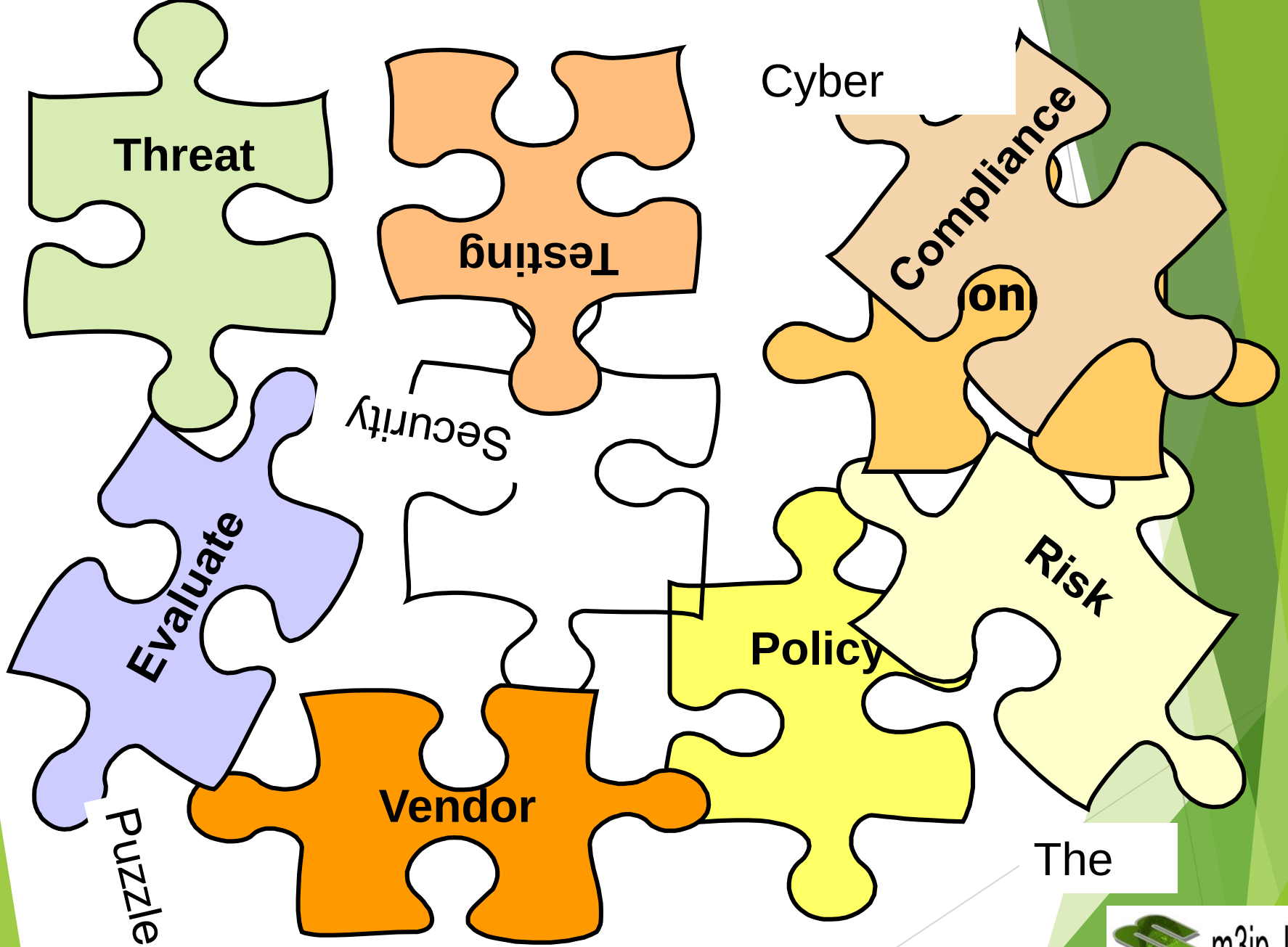


m3ip, Inc.
Managing Your Security And Risk Needs

Cybersecurity Program Puzzle

Identify, Manage & Protect…

m3ip, Inc.
Managing Your Security And Risk Needs



m3ip, Inc.
Managing Your Security And Risk Needs

Cybersecurity Puzzle

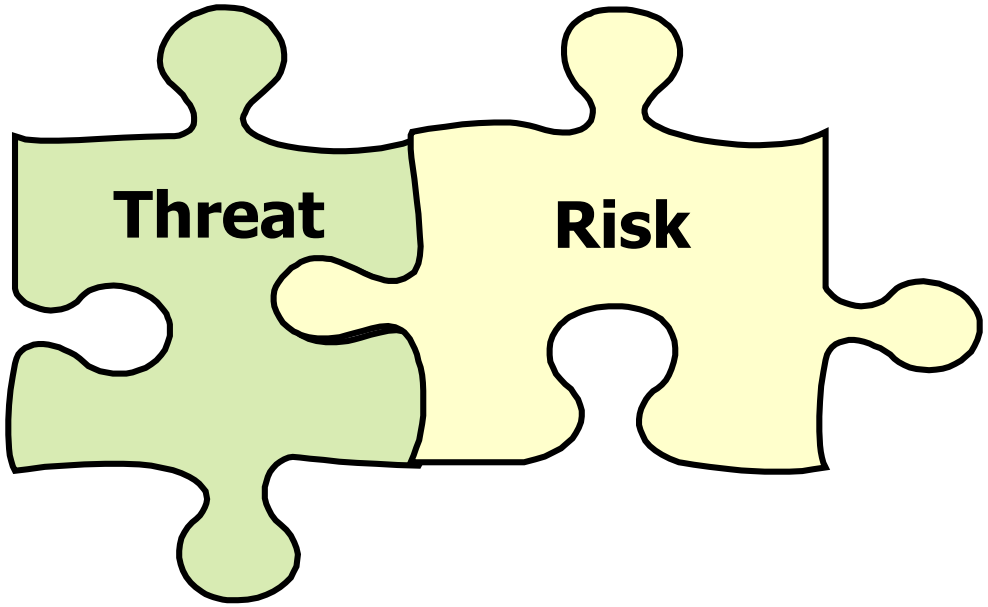
- Understand The Threat:

Inventory

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software

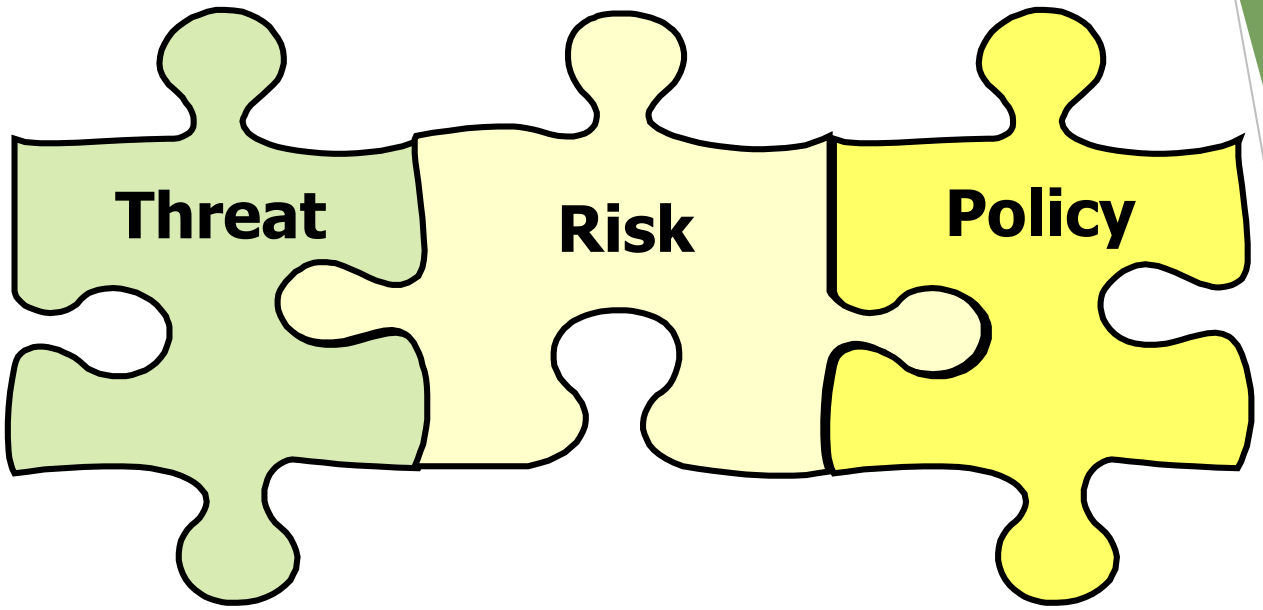
- The first thing an attacker needs is a beach head on your network. Doesn't matter if it's the system with the goods or not.
- Every component on your network is a potential beachhead. Inventorying every thing on your network is a first step to controlling that risk

m3ip, Inc.
Managing Your Security And Risk Needs



- Assess the Risk:
  - Information Technology Risk Analysis
  - Cybersecurity Risk Analysis
  - Business Impact Analysis
  - Cost vs. Risk Tradeoff

m3ip, Inc.
Managing Your Security And Risk Needs

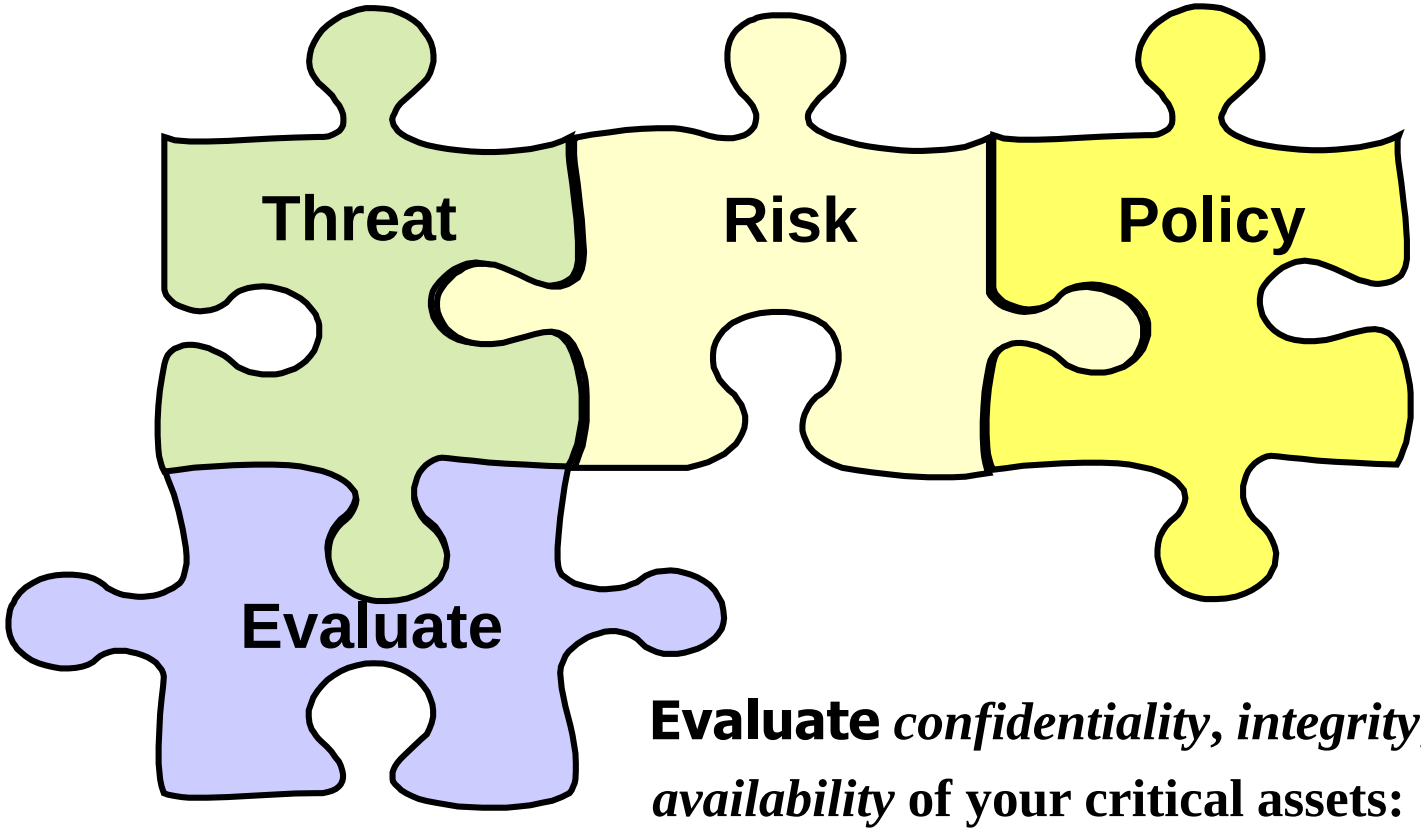


- Develop Policies:

To ensure you **meet your business objectives** and **manage your risk** you need to develop:

- General Information Security Policy
- Specific Functional Security Policy
- Specific Security Procedures and Guidelines

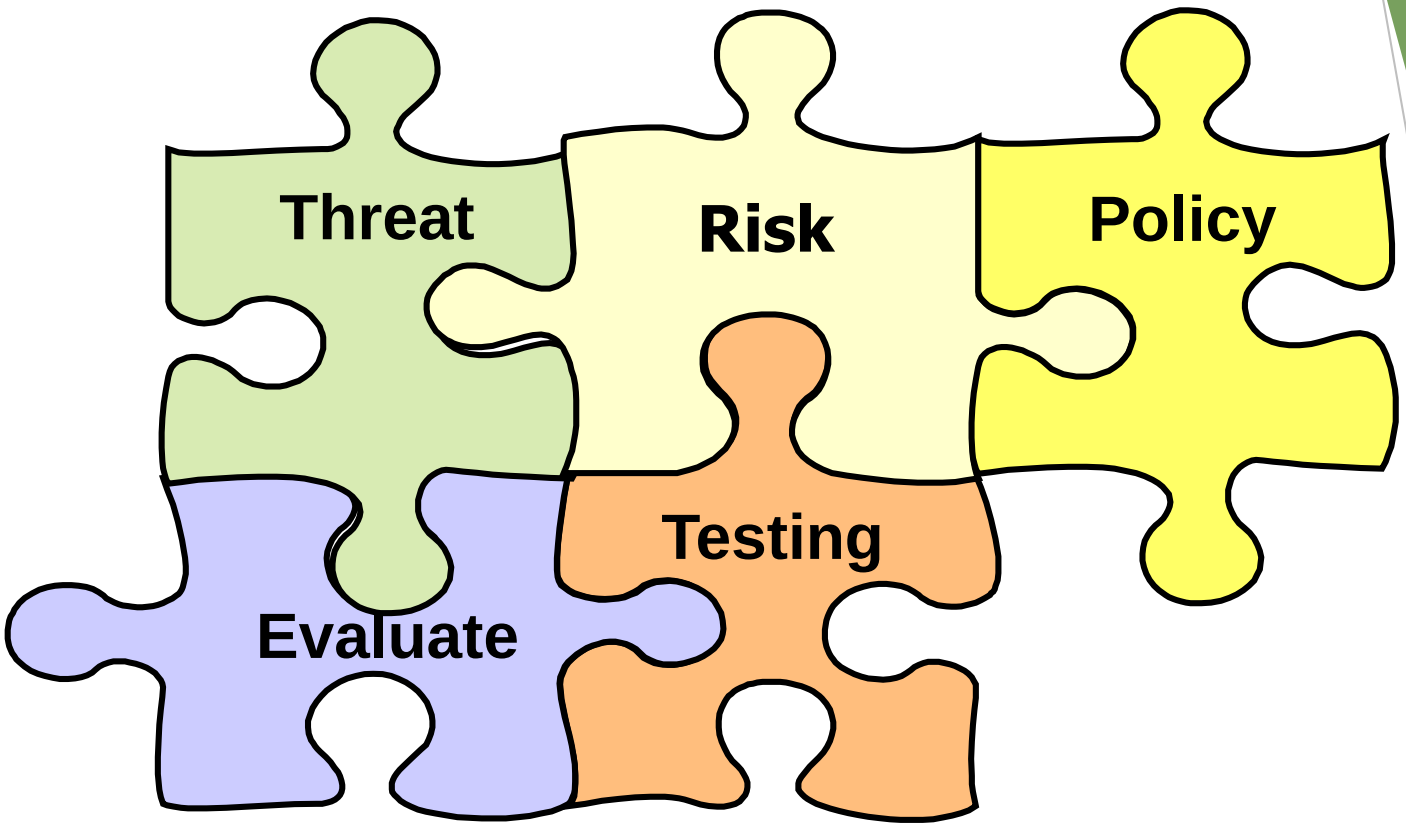
m3ip, Inc.
Managing Your Security And Risk Needs



Evaluate ***confidentiality*****,** ***integrity*****, and** ***availability*** **of your critical assets:**

- Secure State
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Everything authorized on your network has to be secured, whether it has "the goods" or not

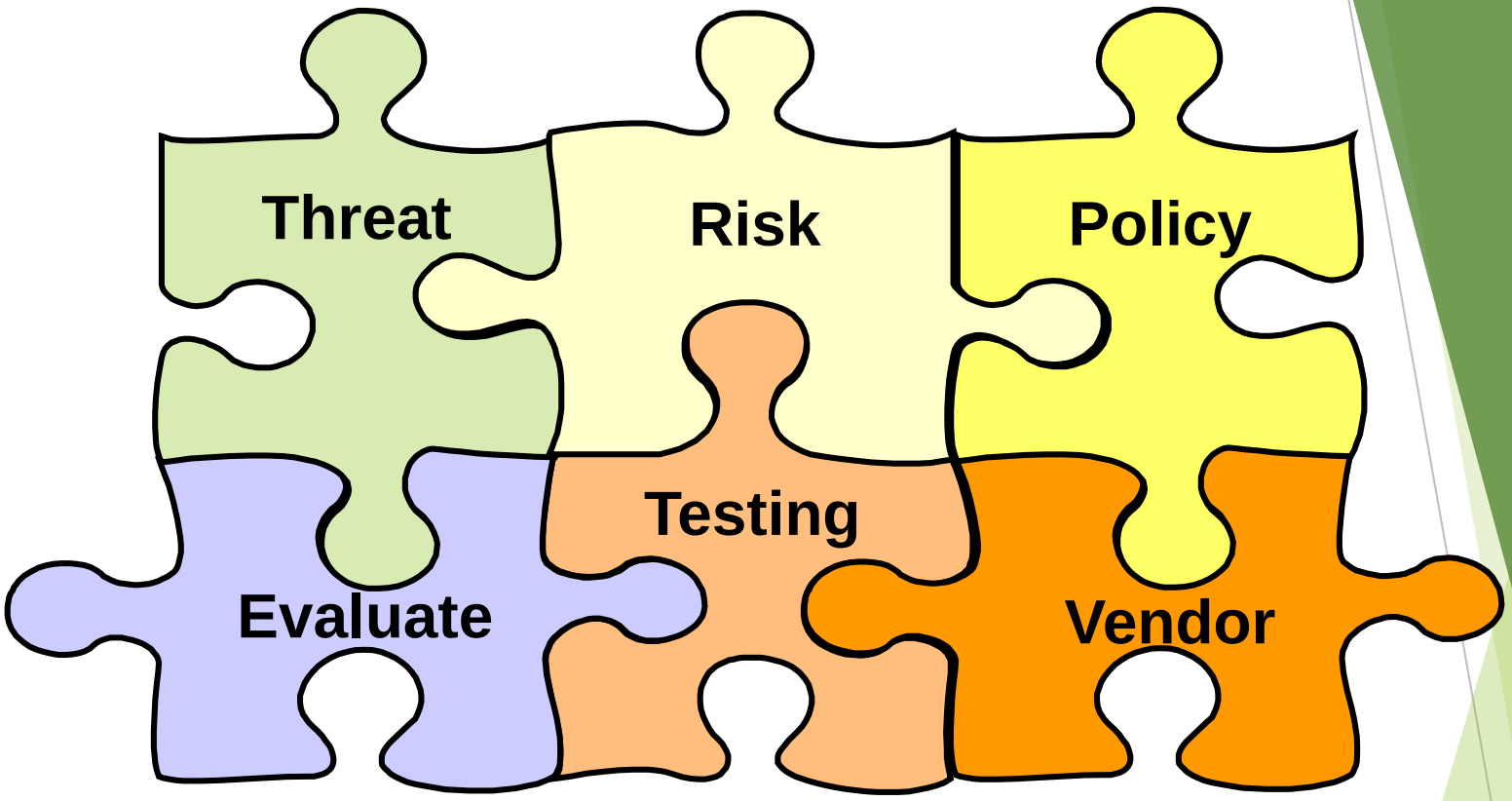
m3ip, Inc.
Managing Your Security And Risk Needs



Vulnerability Management = Fewer Mistakes

- Penetration & Threat Intrusion Testing
- Network Vulnerability Assessment

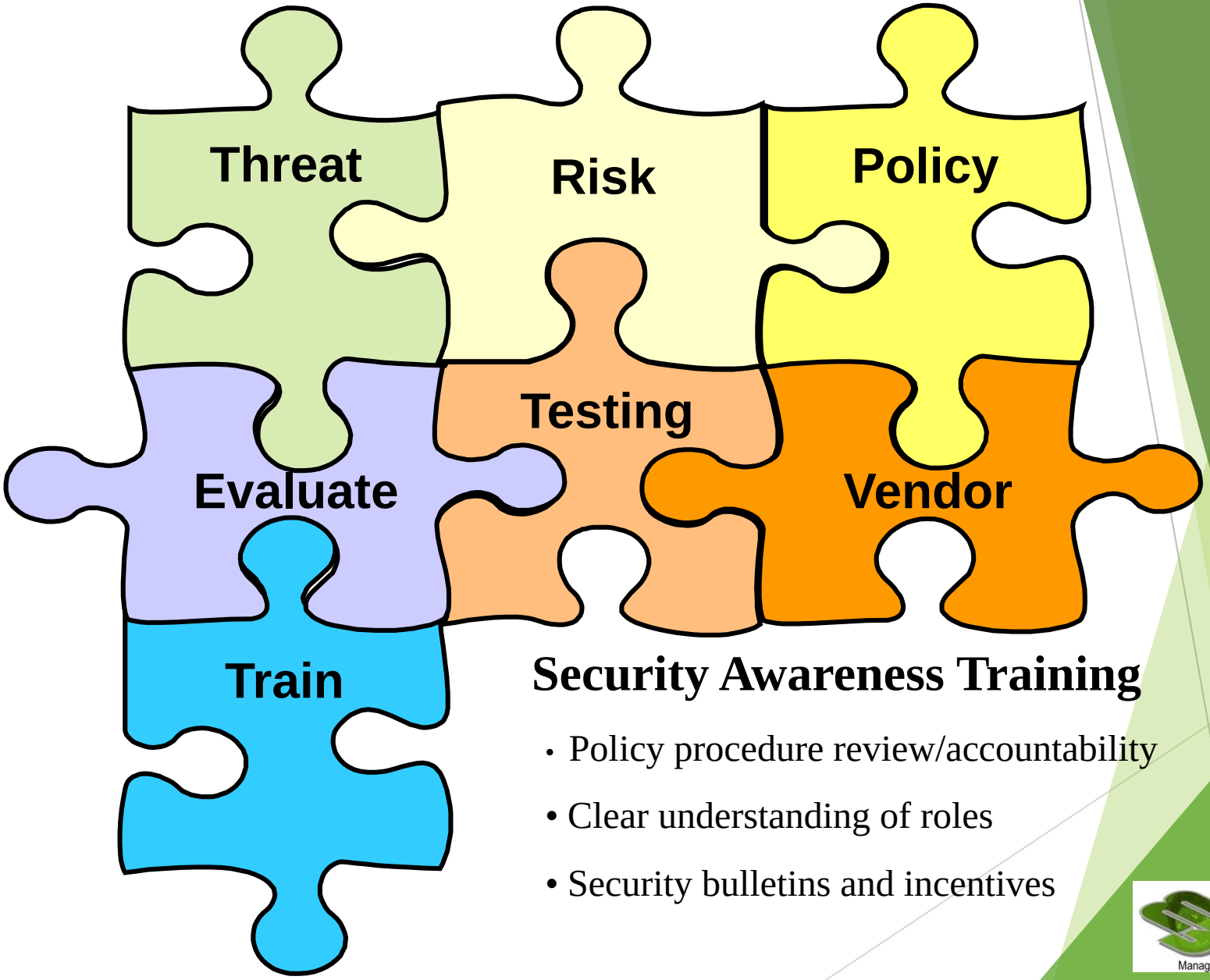
m3ip, Inc.
Managing Your Security And Risk Needs



Vendor Management Program

- Contract Management
- Vendor Classification
- Performance Expectations
- Vendor Oversight

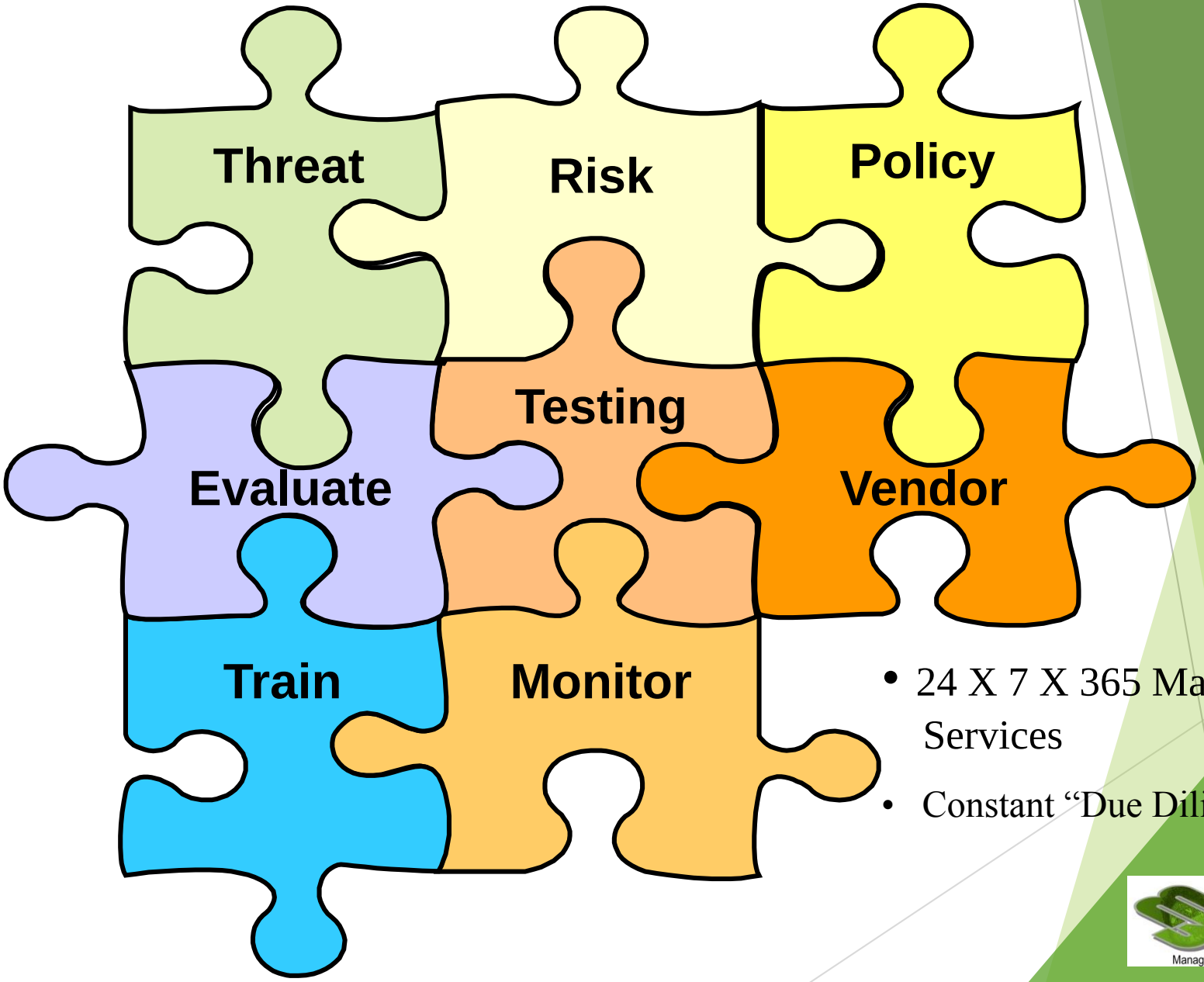
m3ip, Inc.
Managing Your Security And Risk Needs



Security Awareness Training

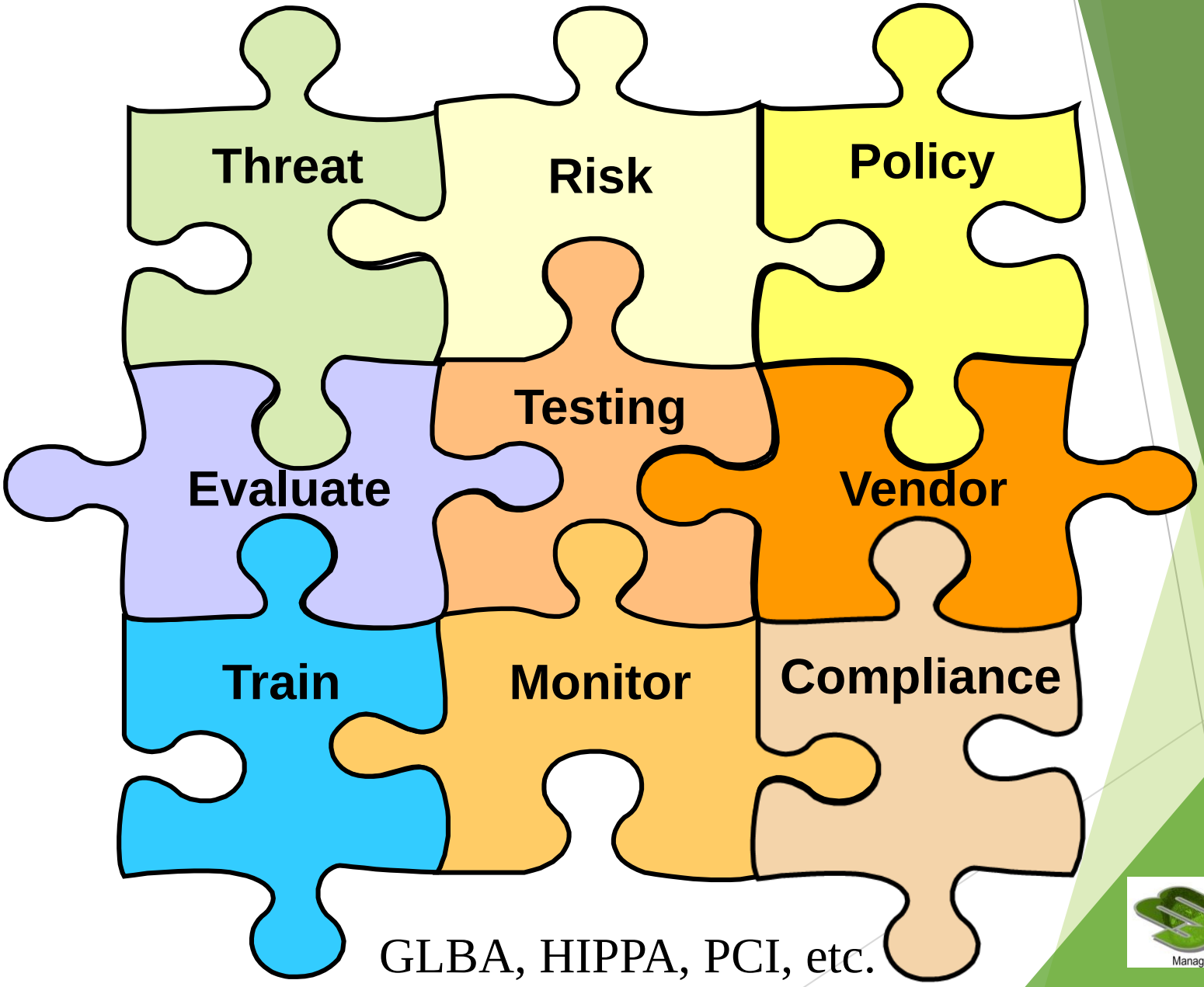
- Policy procedure review/accountability
- Clear understanding of roles
- Security bulletins and incentives

m3ip, Inc.
Managing Your Security And Risk Needs



- 24 X 7 X 365 Managed Services
- Constant “Due Diligence”

m3ip, Inc.
Managing Your Security And Risk Needs



GLBA, HIPPA, PCI, etc.

m3ip, Inc.
Managing Your Security And Risk Needs

Cybersecurity Testing

Things That Go, Bump In The Night…..

m3ip, Inc.
Managing Your Security And Risk Needs

Cybersecurity Testing Challenges

- Shortage of information security technical expertise in many organizations
- Organizations do not have the expertise to perform specialized testing
- Interpreting the results of these tests
- The limitations and improper scope of these tests
- Resource and budget constraints

m3ip, Inc.
Managing Your Security And Risk Needs

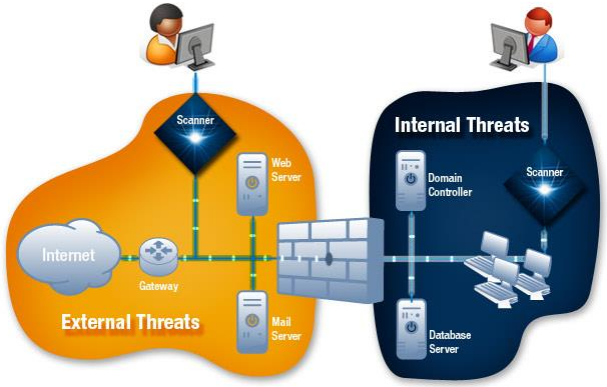
Cybersecurity Testing

- Specialized tests in the cybersecurity area
  - Vulnerability Scans – Automated process of proactively identifying security vulnerabilities of computing systems in a network to determine if and where a system can be exploited and/or threatened
  - Penetration Testing – An attack campaign on a organizations information technology infrastructure conducted by an information security professional with the intention of finding security weaknesses which can be exploited for gaining access to its functionality and data

m3ip, Inc.
Managing Your Security And Risk Needs

Vulnerability Testing

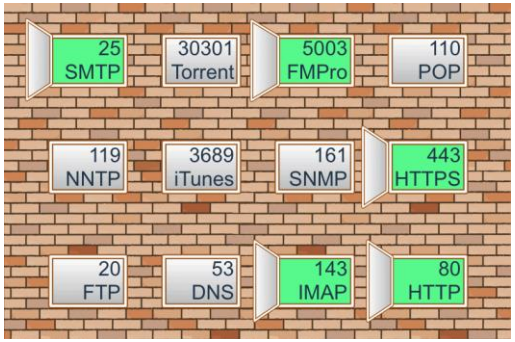
- Internal and External
  - Determine in-scope of the environment
  - Include external critical assets
  - Include disaster recovery sites
  - Include remotes assets, ie laptops, tablets and smartphones used for business purposes



m3ip, Inc.
Managing Your Security And Risk Needs

Vulnerability Testing - continued

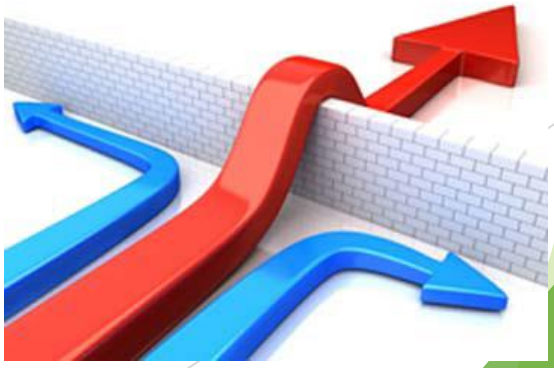
- Discovery
  - Identification of Network Address Segments
  - Operating System Fingerprinting
  - Open Service Ports
    - Test TCP/UDP ports 1-65535
      - Focus on ephemeral ports (OS dependent, i.e. above 1024 for Windows and 32767 for Linux and Unix)



m3ip, Inc.
Managing Your Security And Risk Needs

Penetration Testing

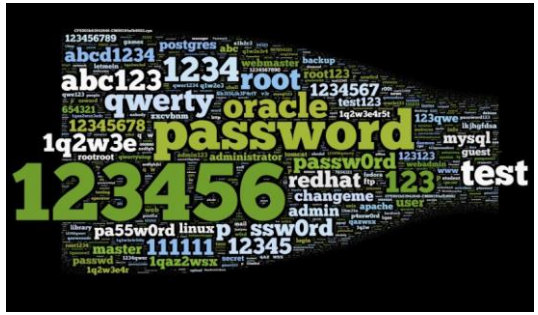
- Vulnerability & Exploit Identification
  - Top Vulnerability Categories
    - Unpatched Applications and Systems
    - Default Credentials
    - Excessive Privileges
    - Unnecessary Services
    - Exposed Web Application Forms



m3ip, Inc.
Managing Your Security And Risk Needs

Penetration Testing - continued

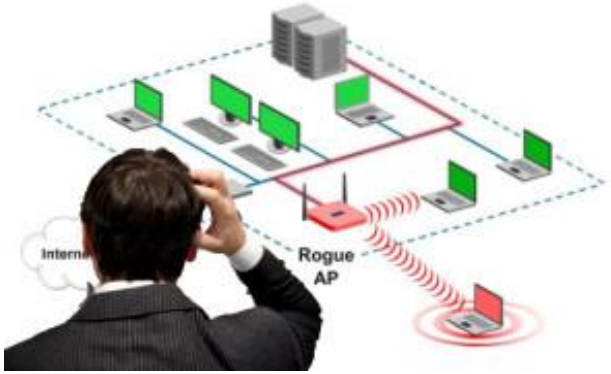
- Credential Manipulation
  - Brute Forcing Passwords
  - Passing The Hash
  - Default Passwords
  - Cookie Harvesting



m3ip, Inc.
Managing Your Security And Risk Needs

Penetration Testing - continued

- Rogue Wireless Access Points
  - User Access To Rogue Device
  - Traffic Interception
  - Key Cracking
  - Cookie Harvesting



m3ip, Inc.
Managing Your Security And Risk Needs

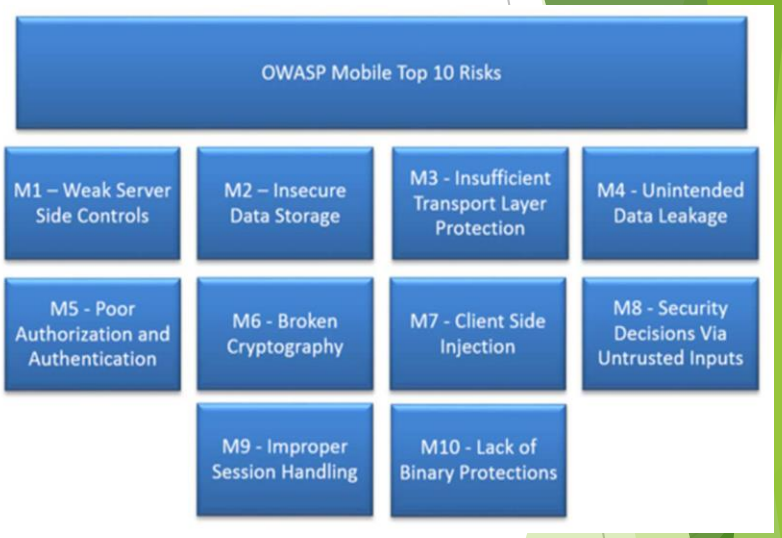
Penetration Testing - continued

- Social Engineering
  - Review On-Line Content
    - LinkedIn
    - Facebook
    - Twitter
    - Instagram
    - Snapchat
  - Custom Campaigns
    - Phishing & Pharming
    - Phone/Text Scams
    - Ruse Customer/Vendor Engagements

m3ip, Inc.
Managing Your Security And Risk Needs

Penetration Testing - continued

- Web Application Testing
  - Identify Roles, Forms & Systems
  - Identify Weaknesses
  - Attempt Exploits
    - Cross-site Scripting
    - SQL Injection
    - Role & Privilege Escalation
    - API Abuse



m3ip, Inc.
Managing Your Security And Risk Needs

Cybersecurity Review

- Information Security Policies & Process
- Risk Assessments
- Security Controls
- Testing Controls
- Continuous Monitoring and Updating

m3ip, Inc.
Managing Your Security And Risk Needs

Cybersecurity Guidelines

- FFIEC Information Technology Examination Handbook (IT Handbook)
  - http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
- Industry accepted cybersecurity best practices (ISO 27002:2013)
  - http://www.informationshield.com/papers/ISO27002%20-%20CyberSecurity%20Framework%20Policy%20Map.pdf

m3ip, Inc.
Managing Your Security And Risk Needs

It Has Been A Pleasure!

- For more detailed information or to schedule an on-site meeting and presentation:

  - Michael Desrosiers

    Founder & Principal

    m3ip, Inc.

    (O)774.992.0985

    (C)774.644.0599

    mdesrosiers@m3ipinc.com

    http://www.m3ipinc.com

m3ip, Inc.
Managing Your Security And Risk Needs

SOPHOS

THE 7 DEADLY I.T. SINS

What are Deadly IT Sins?

Common security pitfalls that are often overlooked...

...putting your network and data at risk!

7 DEADLY I.T. SINS

FAULTY FIREWALL

No.5

What makes a Faulty Firewall?

7 DEADLY I.T. SINS

Bandwidth demands

Social Media

Advanced threats

Poor performance

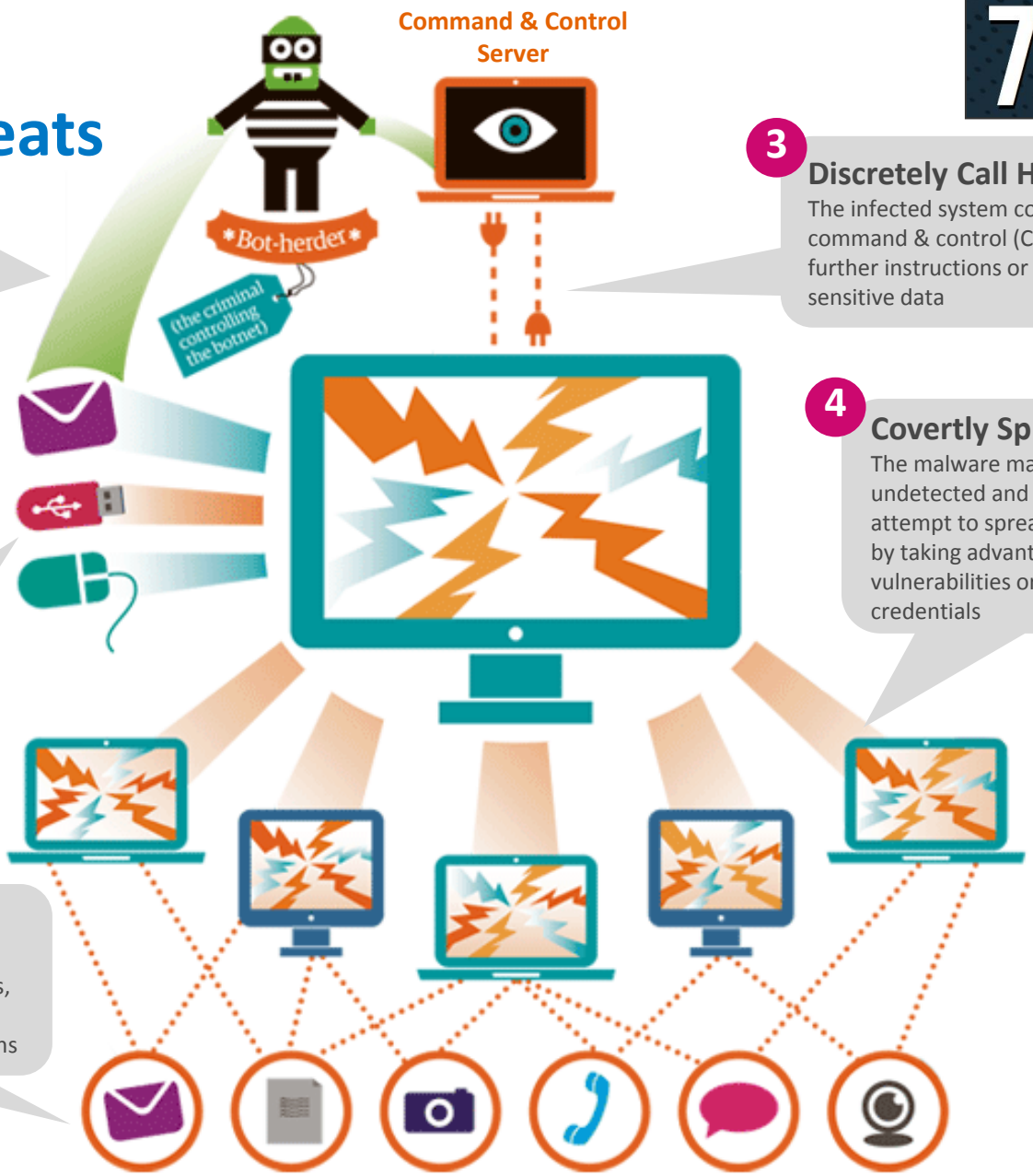
Management complexity

Missing functionality

Limited visibility

Example: Advanced Threats

7 DEADLY I.T. SINS



1 Targeted Attacks

Advanced Persistent Threats (APTs) are usually targeted at specific industries or organizations, but even small businesses can be targeted as well.

2 Entry Point

Targeted or not, the initial system is usually infected by either:

- Visiting an infected website
- Opening an email attachment
- Plugging-in a USB stick

3 Discretely Call Home

The infected system connects to the command & control (C&C) server for further instructions or to start passing sensitive data

4 Covertly Spread

The malware may choose to remain undetected and move slowly or it may attempt to spread to other systems by taking advantage of unpatched vulnerabilities or using hijacked credentials

5 Silently Exfiltrate Data

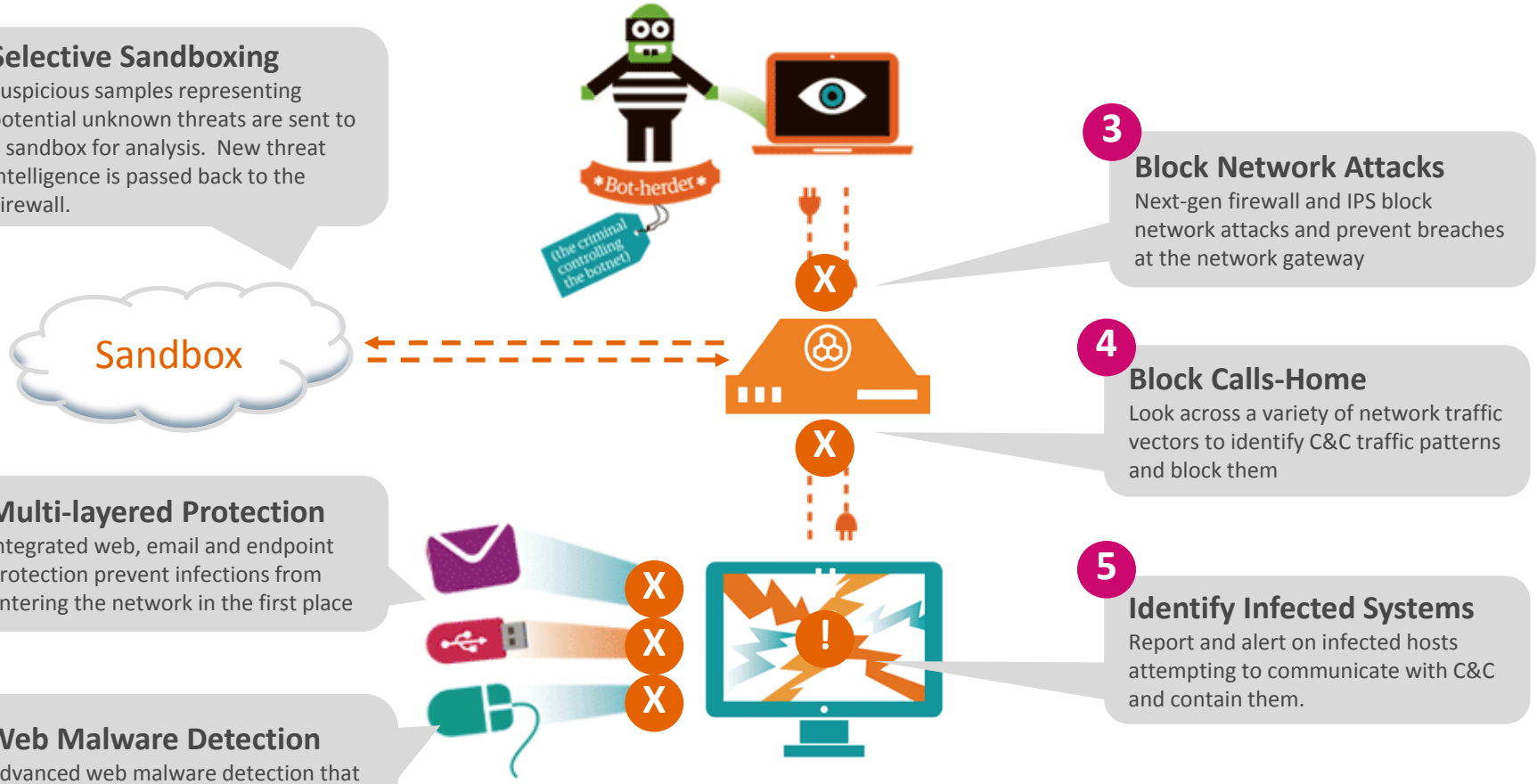
The malware may attempt to steal information from emails, documents, Skype or IM conversations, or even webcams depending on it's intentions

What you need

Preventing, Blocking, Identifying, Sandboxing – Made Simple

7 DEADLY I.T. SINS

6 Selective Sandboxing
Suspicious samples representing potential unknown threats are sent to a sandbox for analysis. New threat intelligence is passed back to the Firewall.



3 Block Network Attacks
Next-gen firewall and IPS block network attacks and prevent breaches at the network gateway

4 Block Calls-Home
Look across a variety of network traffic vectors to identify C&C traffic patterns and block them

1 Multi-layered Protection
Integrated web, email and endpoint protection prevent infections from entering the network in the first place

5 Identify Infected Systems
Report and alert on infected hosts attempting to communicate with C&C and contain them.

2 Web Malware Detection
Advanced web malware detection that can emulate JavaScript to catch even the most sophisticated obfuscated and polymorphic threats

Redemption is here

7 DEADLY I.T. SINS

Your checklist for a new firewall:

1. Usability
2. Performance - real-life scenarios
3. Advanced Protection capabilities
4. Security expertise
5. Reporting

7 DEADLY I.T. SINS

UN-ENCRYPTED FILES

No.6

Un-encrypted Files

7 DEADLY I.T. SINS

Example: Sinfully Unencrypted Laptops

7 DEADLY I.T. SINS

Laptop stolen with health information of 620,000 Albertans

Health officials recently informed of theft from last September

CBC News Posted: Jan 22, 2014 3:30 PM MT | Last Updated: Jan 23, 2014 6:43 PM MT

Stay Connected with CBC News

Mobile Facebook Podcasts Twitter Alerts Newsletter

Latest Edmonton News He

- Plunge in oil price seen as oppo biotech sector 2
- 2 children poisoned by bedbug

Alberta

Stolen Laptops, Hard Drives Expose Over 100,000 People's Personal Data

The data potentially exposed includes names, addresses, phone numbers and Social Security numbers.

By **Jeff Goldman** | Posted February 25, 2015

Share

Several thefts of unencrypted laptops and hard drives recently exposed a significant number of people's personal information.

The Boston Baskin Cancer Foundation recently acknowledged that 56,694 patients' and employees' personal information may have been exposed when an unencrypted external hard drive was stolen from an employee's home on December 2, 2014 (h/t DataBreaches.net).

The drive contained patient demographic information, birthdates, Social Security numbers, phone numbers and first and last dates of clinic visits for patients seen between 2008 and July 2014. For employees, the drive held titles, office locations, Social Security numbers, birthdates, pay rates, and dates of employment.

Coca-Cola Says 74,000 Affected After Company Laptops Stolen

Coca-Cola's shares fell 1 percent to $38.84 at the close in New York and added 14 percent last year. Photographer: Dario Pignatelli/Bloomberg

Redemption the easy way

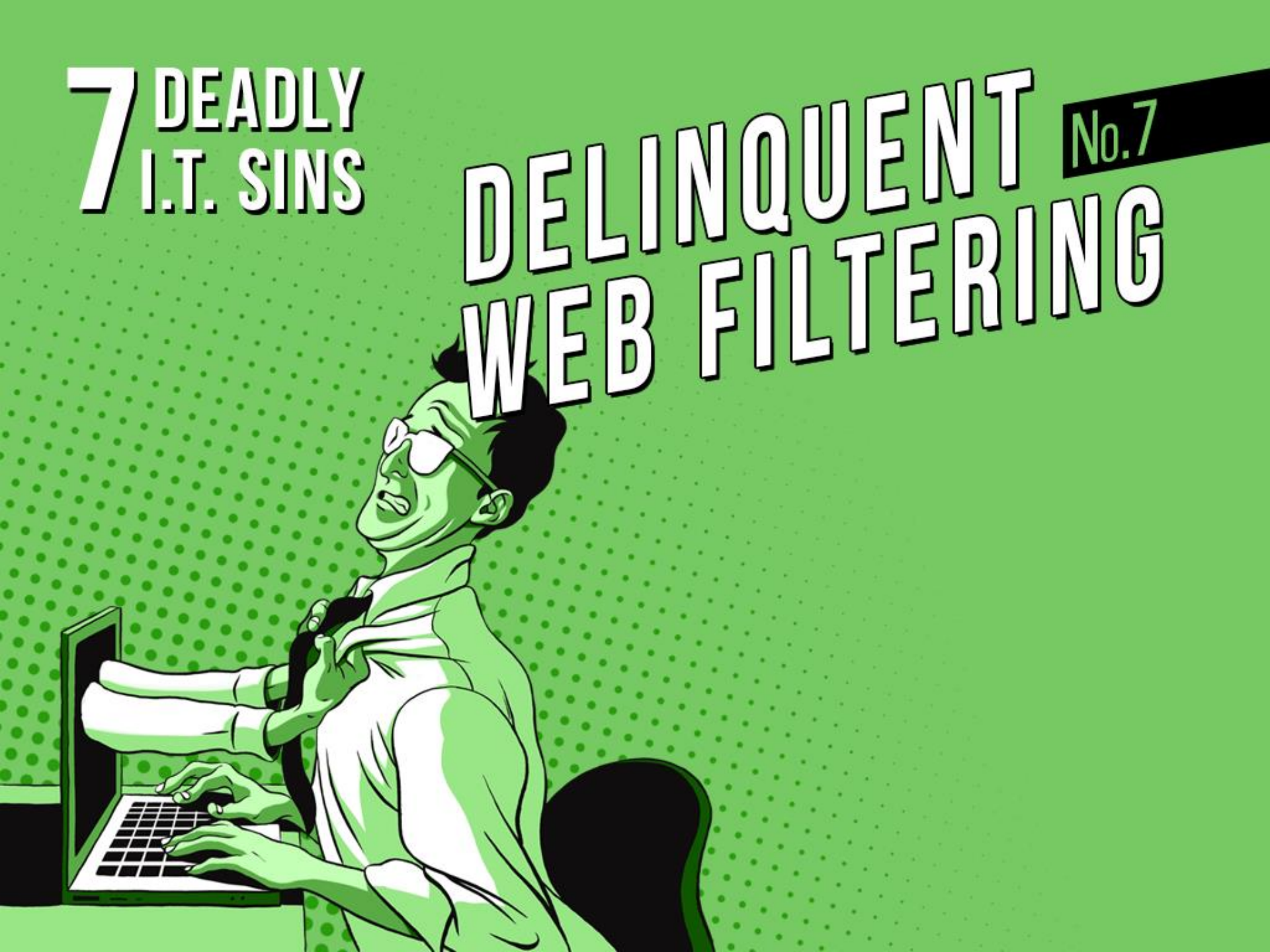
7 DEADLY I.T. SINS

Your checklist for encryption:

1. Use full-disk encryption on all laptops
2. Use server encryption
3. Encrypt your email (see Sin #4)
4. Implement file encryption across cloud and mobile devices
5. Reporting, Management, Auditing

7 DEADLY I.T. SINS

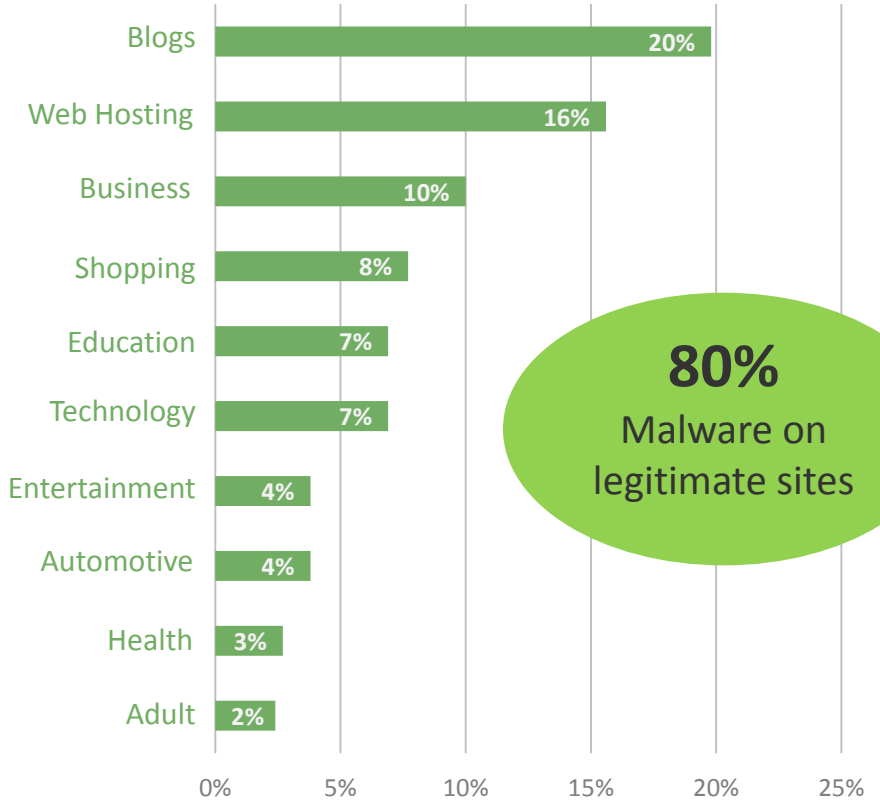
No.7 DELINQUENT WEB FILTERING



Delinquent Web Filtering

7 DEADLY I.T. SINS

Top 10 infected web site categories



80%
Malware on legitimate sites

40,000
New web threats every day

$400M
Stolen through GameOver malware

Example Web Attack

7 DEADLY I.T. SINS

Entry Point

Drive-by-download from a hijacked website or an email with a malicious link

Distribution

Initial malware redirects based on what it's working with (Windows/Mac, IE/Safari, Java)

Exploit

Exploit pack attempts to leverage a number of vulnerabilities

Infection

Download of a malicious payload

Execution

Malware calls home with sensitive data

TMZ.com

The New York Times

Spotify

London Stock Exchange

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java Rhino ›	1985	96.88
MDAC ›	28	1.37
PDF ALL ›	12	0.59
PDF LIBTIFF ›	10	0.49
HCP ›	9	0.44
Java OBE ›	5	0.24

Exorcising Delinquent Web Filtering

7 DEADLY I.T. SINS

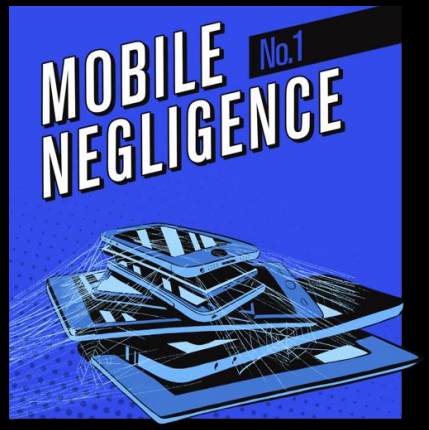
Web Security Checklist:

- Spam filtering
- Real-time URL reputation filtering
- Web malware scanning
  - JavaScript emulation
  - Behavioral Analysis
- HTTPS Scanning
- Advanced threat detection
- Real-time cloud updates
- Business-grade AV with HIPS

+ Protection Everywhere Users Go!

Know them. Fear them. Fix them.

7 DEADLY I.T. SINS

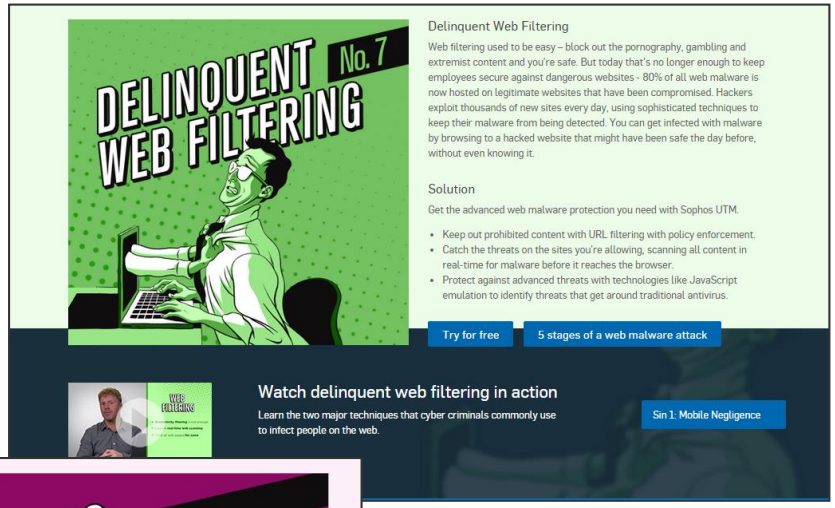


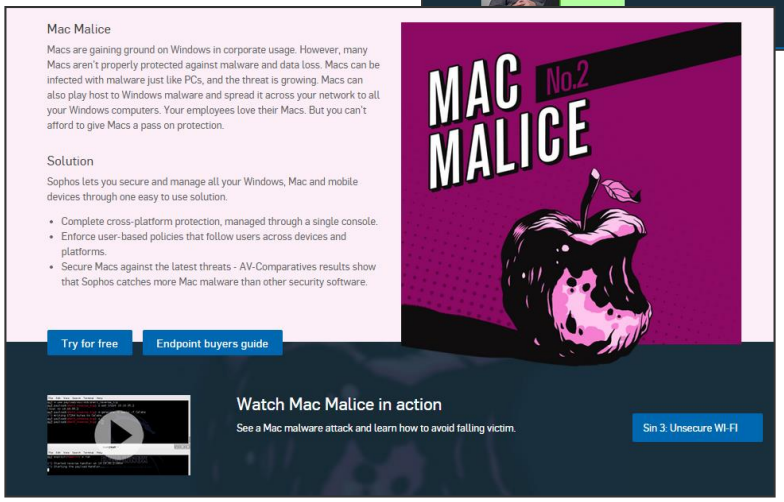
SOPHOS

How Sophos can help

www.sophos.com/sevensins

- Learn more about each Sin
- Watch 90 second video, including hack demos
- Read useful whitepapers
- Try solutions for free





Why Sophos

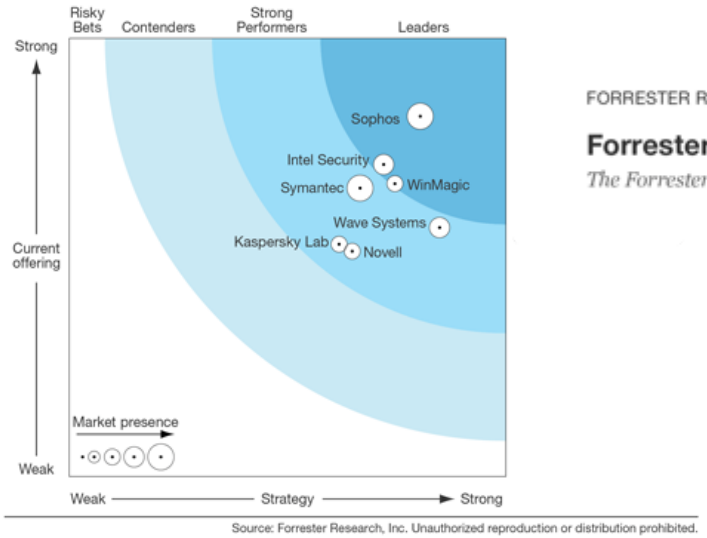
1985
FOUNDED

200,000+
CUSTOMERS

100M+
USERS

22 Offices
GLOBALLY

- SophosLabs global threat detection network
- Gartner Leaders for Endpoint, Encryption and UTM
- ‘Breakout star’ in Forrester Encryption Wave 2015



FORRESTER RESEARCH | SECURITY & RISK PROFESSIONALS

Forrester Wave™: Endpoint Encryption Market, Q1 2015

The Forrester Wave™: Endpoint Encryption, Q1 2015

BizCompass

Maines Technology Leader in Managed Services

InformationTechnology CloudHosting DataProtection

Is my cloud secure?

Definition of Cloud

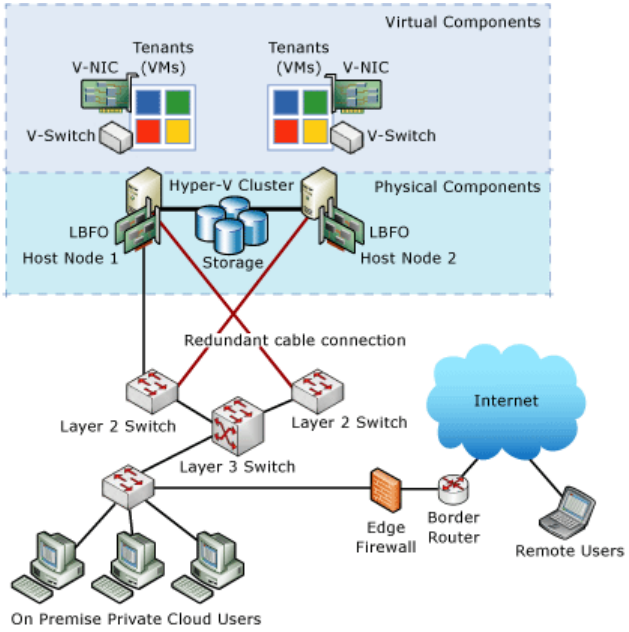
- On-Demand Network Access
- Shared Pool of Computing Resources Like
  - Network, storage, servers, applications and services
- Accessible from any Internet enabled device
- Offers many services from email to financial applications
- Platforms
  - IaaS – Infrastructure as a Service
  - Saas – Software as a Service
  - PaaS – Platform as a Service

Types of Clouds

- Private Cloud - The infrastructure is provisioned for exclusive use by a single organization
  - Dedicated server for client applications like QuickBooks
- Public Cloud - The infrastructure is provisioned for open use by the general public
  - Google, DropBox, Amazon
- Hybrid Cloud - The infrastructure is a composition of two or more distinct cloud Infrastructures
  - Hosted Exchange email with dedicated servers for client applications

Cloud Infrastructure

- Cloud and Virtualization is Delivered in Layers
- The Physical Components
- The Virtual Components
- The Network Infrastructure
- The Internet Provider
- !!!! The Security !!!!



Assessing Risk being on the ~~Cloud~~/Internet

- Hackers target big business!!! – NO!
- Where is your data?
- Who has access to your data?
- Transient security risk?
- Third party access?
- What is my biggest risk?
- I have virus protection!
- Ransom Ware

Choosing Your Cloud

- Stay Local
- Know where your data is
- Hire the professionals
- How will you connect (private connection)
- How will your data be migrated
- Talk to references
- What is the backup strategy
- Exit strategy

What is at Risk?

- Data – Data is stolen without knowledge
- Corporate Intellect – What can competition do with your intellectual data
- Reputation – Just the breach alone
- Partnerships – Data interconnects are vulnerable
- Client data – You must alert your clients
- Monetary Risk – Someone has to pay

How to Protect Yourself

- Keep sensitive data out of public cloud services (DropBox, Google, Etc.)
- Encrypt your data in transit and in storage
- Keep passwords strong
- Do not share user accounts
- Keep firewalls turned on when using public hot spots
- Use A/V on Smartphones and Tablets
- Typing passwords in public is easy prey
- Keep Anti-Malware/Virus current
- If your computer acts strange likely should be scanned
- Follow your instinct
- Listen to what your computer is telling you
- !!!!!!! Take TWO !!!!!!!!!!!!!!!
  - Dissect information, grammar, spelling, appropriate?
- Click happy????!!!!

Technology That Helps Protect You

- UTM – Unified Threat Management Appliance
- Firewall – Old School
- End Point Protection
- Anti-Virus and Anti-Malware Software
- End User Education
- Data Encryption Software
- Data Leak Protection
- Email Scrubbing
- Corporate Use Policy

Berry · Talbot · Royer

CERTIFIED PUBLIC ACCOUNTANTS

BTR

"Big enough to serve, small enough to care"

Applying the COSO Framework to Cyber Risks

CYBER RISKS CANNOT BE AVOIDED OR ELIMINATED

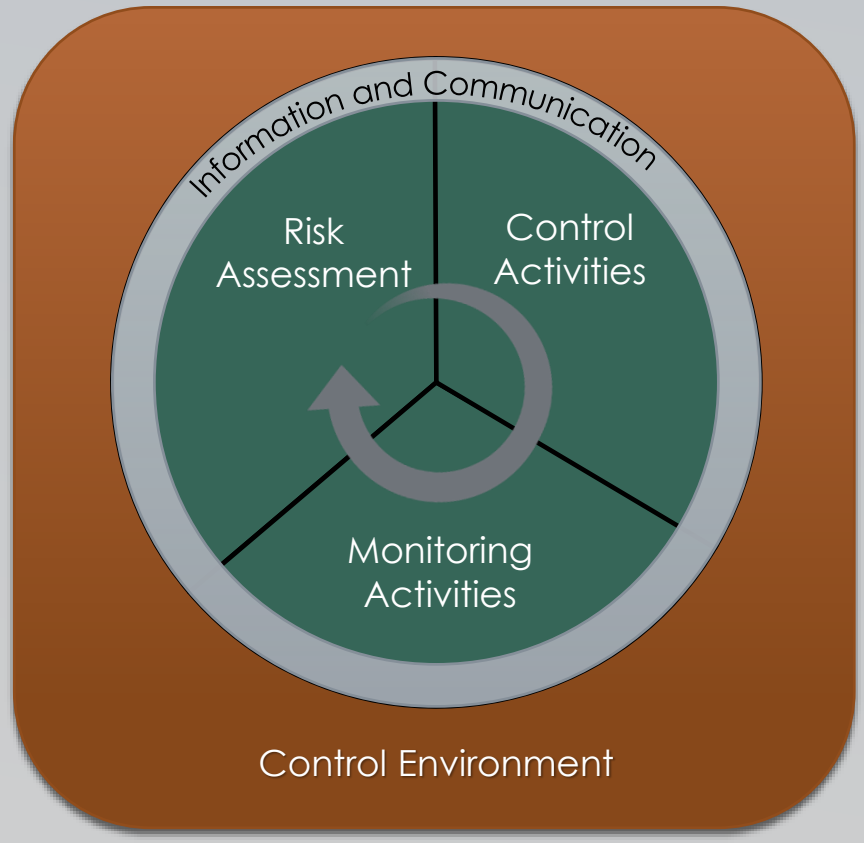
- All organizations must use IT systems to keep pace with society
- Technology keeps evolving
- Methods of attack and exploitation are relentless and constantly adapting.

Therefore, the risks must be continually managed.

BTR

The COSO *Internal Control – Integrated Framework* can help you manage risks in an efficient and effective manner.

Five Components of the *Framework*



- Ongoing and iterative process
- Applied to objectives to manage risk
- Implemented across all levels of the organization

What are the organization's objectives?

- The Board and senior management set long-term objectives.
- Operational management and area specialists determine focused objectives that contribute to the organization's overall objectives.
- Objectives are divided into three categories:
  - Operational objectives
  - Reporting objectives (financial/non-financial, and internal/external)
  - Compliance objectives

RISK ASSESSMENT

Clearly specify objectives
Identify risks at all levels, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

Which information systems would prevent achievement of objectives if they were disrupted, degraded, or destroyed?

- Identify information systems that are used in achieving organizational objectives.
  - Operating objectives
  - Reporting objectives
  - Compliance objectives
- Specify how each information system contributes to organizational objectives.
  - Collaboration and consultation with IT specialists is necessary
- Assign a value to each information system
  - Organizations have limited resources
  - Valuing information systems allows the organization to determine criticality
  - Often an IS's value is related to other non-IS critical assets

RISK ASSESSMENT

Clearly specify objectives
Identify risks, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

The end result of this step:

- A list of specific objectives
- An inventory of information systems mapped to objectives
- A ranking of information systems by their value to achieving objectives

Value	System	Objective A	Objective B	Ojective C	Objective D
10	**Information System A**	Performs x function to accomplish y results	Performs x function to accomplish y results	Performs x function to accomplish y results	N/A
8	**Information System B**	N/A	Performs x function to accomplish y results	N/A	Performs x function to accomplish y results
8	**Information System C**	N/A	Performs x function to accomplish y results	Performs x function to accomplish y results	N/A
5	**Information System D**	N/A	N/A	N/A	Performs x function to accomplish y results
3	**Information System E**	N/A	N/A	Performs x function to accomplish y results	N/A

RISK ASSESSMENT

Clearly specify objectives
Identify risks, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

How can the information systems be disrupted, degraded, or destroyed?

- This is a brainstorming session with senior management, operational management, and area specialists.
- Requires an understanding of an attacker's likely motivations and tactics.
  - What data do you have that attackers might want?
  - What vendors, customers, or employees do you have that attackers might want to exploit?
  - What objectives do you have that attackers might want to obstruct?
  - How will attackers likely attack?
- Be as specific as possible in describing the risk (who, what, when, where, why, & how)
- Risks **also include changes** either internally or externally that could affect controls
  - Employee turnover
  - Changes to processes and technology
  - Changes in the external environment (economy, politics, social changes, etc.)

RISK ASSESSMENT

Clearly specify objectives
Identify risks, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

The end result of this step:

- A list of specific risks
- A mapping of the risks to information systems

Risk ID	Risk Description	Info Sys A	Info Sys B	Info Sys C	Info Sys D	Info Sys E
Risk A	AA could infiltrate ZZ by XX means and steal YY data.		X	X		
Risk B	Collusion among employees could cause PP to be fraudulently corrupted.				X	X
Risk C	Natural disaster CC could destroy RR data.	X	X	X		X
Risk D	QQ data could be manipulated to result in errors for GG customers.	X	X		X	

RISK ASSESSMENT

Clearly specify objectives
Identify risks, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

Which identified risks are the highest risks and which are the lowest?

- Determine each identified risk's likelihood
  - Remote 0 – 15% chance of occurrence
  - Unlikely 15 – 35% chance of occurrence
  - Even Chance 35 – 65% chance of occurrence
  - Probable 65 – 15% chance of occurrence
  - Almost Certain 85 – 100% chance of occurrence
- Determine each identified risk's potential severity (this is tied to the information system's value)
  - Minor 1 – 2 on a scale of 1 - 10
  - Moderate 3 – 7 on a scale of 1 - 10
  - Major 8 – 10 on a scale of 1 - 10
- Rank the risks using the combined scores of likelihood and severity

RISK ASSESSMENT

Clearly specify objectives
Identify risks, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

The end result of this step:

- A ranking of the identified risks

Risk ID	Likelihood	Severity	Risk
Risk A	60%	2	1.2
Risk B	40%	9	3.6
Risk C	10%	3	0.3
Risk D	90%	6	5.4

The end result of the Risk Assessment phase:

- A list of specific objectives
- A ranked inventory of information systems, mapped to objectives
- A ranked inventory of identified risks, mapped to information systems

RISK ASSESSMENT

Clearly specify objectives
Identify risks, including fraud risks, to achieving those objectives
Analyze the identified risks for likelihood and severity

- Given limited resources, start with the most critical risks to the most valuable information systems.
- Create a layered approach to control activities so that there isn't simply one layer of defense to be penetrated
- Use a combination of detective controls and preventive controls
  - Preventive controls are designed to keep attacks from be being realized.
  - Detective controls are designed to identify breaches *in a timely manner* so that corrective action and damage assessment can be conducted as soon as possible.
- There should be a mix of General Information Technology Controls, specific Application Controls, and general business controls.
- Collaborated and use IT specialists expertise in designing these controls.

CONTROL ACTIVITIES

Select and develop control activities to respond to risks
Implement activities through policies and procedures

BTR

- Documentation and training are crucial for controls to be implemented correctly
  - Document which employees/positions are responsible for performing control activities
  - Communicate to employees the risks being controlled for by specific control activities
  - Train employees on how to perform their assigned control activities
  - Document how to conduct the control activities and the frequency with which they're to be applied
- For automated controls, ensure documentation includes how the automated control functions, who has authorized access to the underlying code of the controls and how changes may be made, runs of test data and expected outputs, how notification of breaches is relayed, and who is responsible for responding to notifications
- For controls performed by service organizations, ensure policies exist on service organization qualifications, inputs to the service organization and expected outputs (including in-house controls over inputs and outputs), and periodic assessments of service organizations.

CONTROL ACTIVITIES

Select and develop control activities to respond to risks
Implement activities through policies and procedures

BTR

- Monitoring activities should be aimed at the whole system of internal control, not just control activities.
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring Activities
- Internal monitors should maintain objectivity and a certain level of independence.
- When monitoring control activities, determine the following:
  - Are the controls designed effectively? Will the controls actually reduce any risk?
  - Are the controls operating effectively? Are the controls being performed competently and consistently by the person authorized to perform them?

MONITORING ACTIVITIES

Select, develop, and perform activities to determine internal control components are present and functioning
Evaluate and communicate internal control deficiencies

BTR

- An internal control deficiency is a shortcoming in any of the components of internal control or their relevant principles that reduces the likelihood of achieving objectives.
- Internal control deficiencies should be assessed for potential impact on the entire system of internal control.
- A *major deficiency* severely reduces the likelihood of achieving objectives.
  - If one or more of the component principles are not *present and functioning*, a major deficiency automatically exists.
  - When a major deficiency exists, the system of internal control is not effective.
- Procedures and communication lines should be in place to report deficiencies to senior management and the board in a timely fashion so that they can be corrected.

MONITORING ACTIVITIES

Select, develop, and perform activities to determine internal control components are present and functioning
Evaluate and communicate internal control deficiencies

BTR

Information and Communication

This component is *interwoven* among all the other components. So elements of it are seen in each area.

The organization must be able to obtain or generate quality information.

- Quality information is **relevant** and **reliable**

Information is necessary to support the functioning on internal control.

Communication of information must be sent to and received by necessary internal or external stakeholders in a timely manner.

Control Environment

This component is the *foundation* of all other components. It's the environment that permits the rest of the components to exist and function.

The organization establishes a sound environment by

- Demonstrating a commitment to integrity and ethical behavior
- Demonstrating independent oversight of management by the Board
- Establishing effective structures, reporting lines, and authorities and responsibilities
- Demonstrating a commitment to attract, develop, and retain competent individuals
- Holding individuals accountable for their responsibilities

Q & A

PROTECT YOUR DATA. ASSESS YOUR RISK.

Berry · Talbot · Royer
CERTIFIED PUBLIC ACCOUNTANTS

SOPHOS

BizCompass
Maines Technology Leader in Managed Services
InformationTechnology CloudHosting DataProtection

---

m3ip, Inc.
Managing Your Security And Risk Needs

PATCO Construction, Inc.