

CyberRisk Solutions Threat Landscape and Strategic Operations Overview



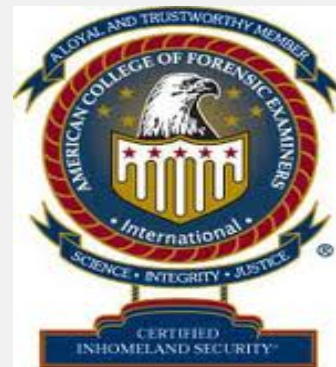
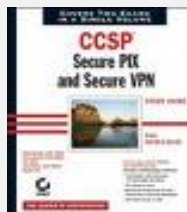
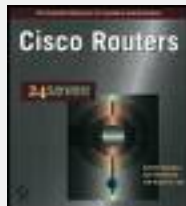
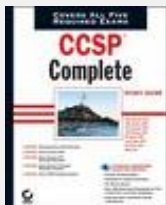
About Bryant G. Tow, Managing Partner



Distinguished
Fellow



President, Mid-TN
VP National (former)

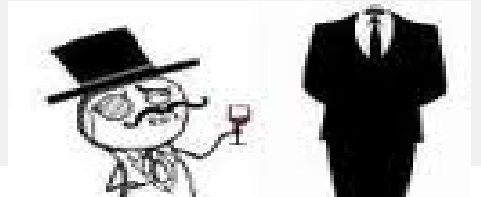




- Cyber Threat Landscape
- CyberRisk Solutions Overview
- CyberRisk Solutions Services



Cyber Threat Landscape





<https://youtu.be/FYUjvbaj4bo>

UNITED CYBER CALIPHATE

NOW

TOGETHER

GHOST
CALIPHATE SECTION



SONS
CALIPHATE ARMY



CALIPHATE
CYBER ARMY



Kalachnikov
E-security team



YOUR BROWSER HAS BEEN 

fbi.gov.id130873813-8342929103.z3476.com

THE FBI CYBER DEPARTMENT
FEDERAL BUREAU OF INVESTIGATION



All activities of this computer have been recorded
All your files are encrypted. Do not try to unlock your computer!
Your browser has been blocked due to at least one of the reasons specified below.

You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.
Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of Portugal, provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to \$100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and avoid other legal consequences, you are obligated to pay a release fee of \$300, payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with \$300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?



Your IP: 
Location: **San Francisco, California, United States**

 **MoneyPak** SECURE PAYMENT FORM

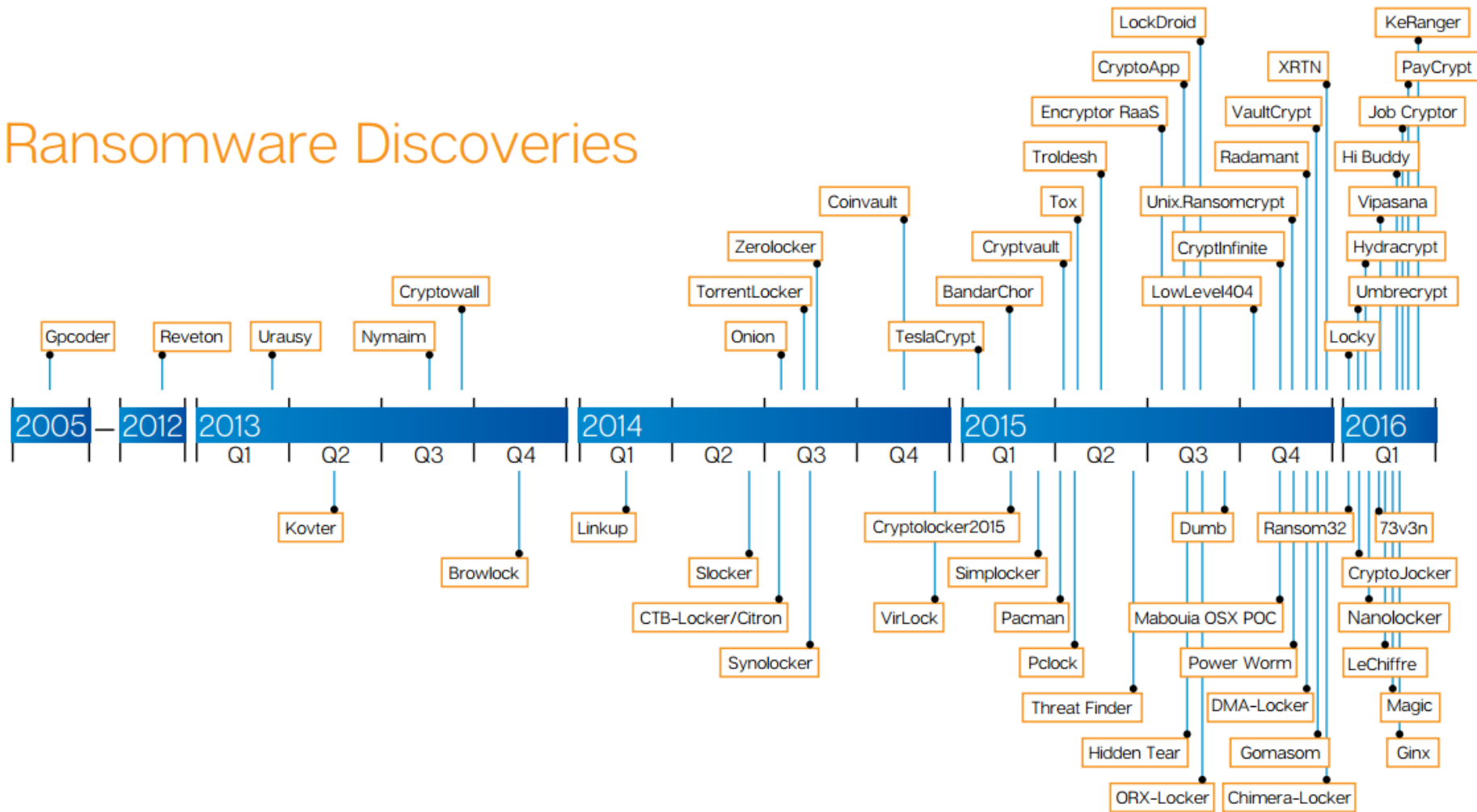
Enter the MoneyPak code

Please enter MoneyPak code using pin pad below.

1 2 3 4 5 6 7 8 9 0 Clear

UNLOCK YOUR PC NOW!

Ransomware Discoveries





Phoenix Division

Select Language

Get FBI Updates

[Home](#) • [Phoenix](#) • [Press Releases](#) • 2016 • [FBI Warns of Dramatic Increase in Business E-Mail Scams](#)

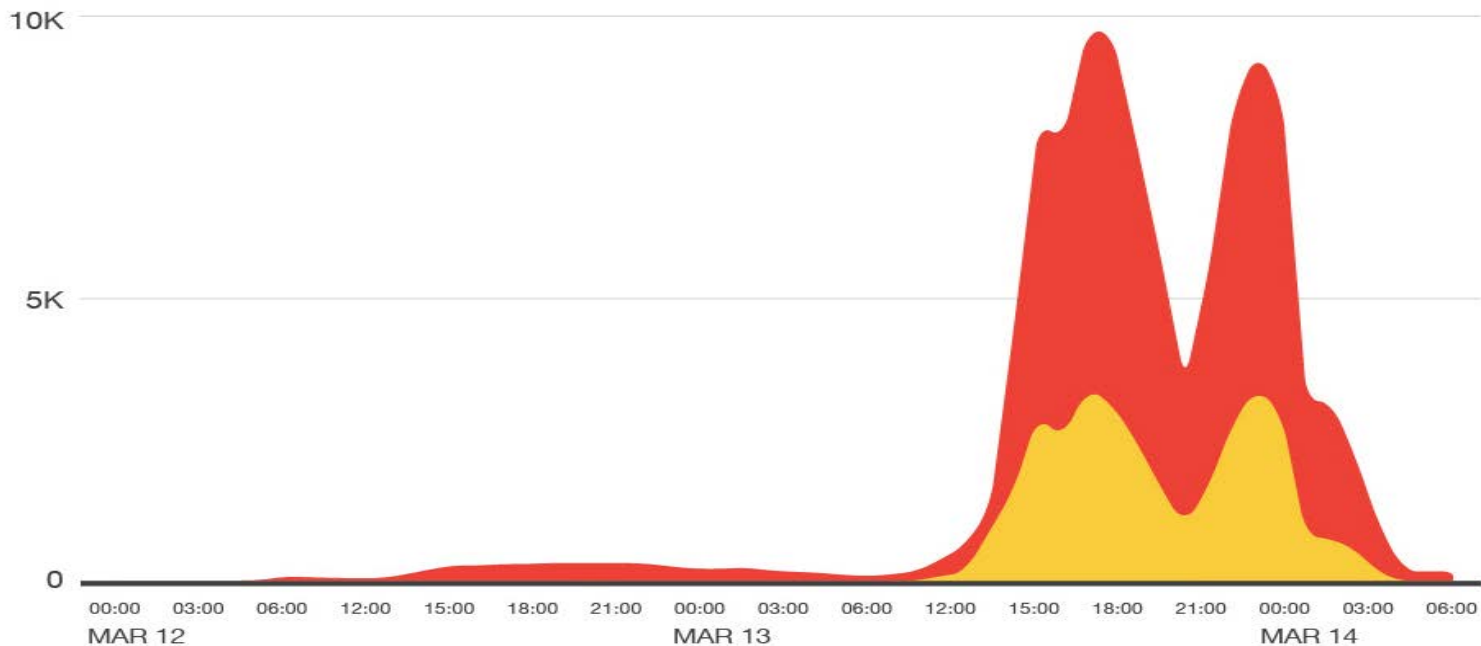
- Law enforcement globally has received complaints from victims in every U.S. state and in at least 79 countries.
- From October 2013 through February 2016, law enforcement received reports from 17,642 victims.
- This amounted to more than \$2.3 billion in losses.
- Since January 2015, the FBI has seen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

Malvertising servers used in this attack, and corresponding activities in the last 24 hours (UTC)



#	Result	Protocol	Host	URL	Comments	Body
5	200	HTTP		/tracker?zone=1456&camp=	Malvertising	2,468
8	200	HTTP		/track/k.track?wd=48&fid=2&rds=b1714032cd63652bc95fadf5dc81da...	Malvertising	1,096
9	200	HTTP		/topic/55879-mash-crested-interdepartmental-boat-encomium-tabulati...	Angler Exploit Kit	150,050
10	200	HTTP		/topic/55879-mash-crested-interdepartmental-boat-encomium-tabulati...	Angler Exploit Kit	2,424
11	404	HTTP		?o=SeU8W&j=&l=8Nax-ID&k=Kq6T&y=hSn4v4c2&v=IOUdQbcD&q=...	Angler Exploit Kit	5
12	200	HTTP		?o=SeU8W&j=&l=8Nax-ID&k=Kq6T&y=hSn4v4c2&v=IOUdQbcD&q=...	Angler Exploit Kit	37,486
13	200	HTTP		?y=&j=Q0kw7fJ&e=&k=SmlFhY4nRe&u=8G5yK9&t=&g=SEyksUn&o=...	Angler Exploit Kit	101,347
15	200	HTTP		?l=z7yS6K5&b=&x=P8q&k=&i=PXj&s=&t=Zf38qkob9&c=&y=Kffry4R...	Angler Exploit Kit	689,612
23	200	HTTP				72,785
24	302	HTTP				5
25	302	HTTP				76
26	200	HTTP				39
27	200	HTTP				378
28	200	HTTP		/?j=JZtiqVAAD0&q=S_4EvUNzgo&g=ECwoWi&w=WeeoWS&y=Wt4&l=...	Angler Exploit Kit	333,511
29	200	HTTP				689,612
37	200	HTTP				249
38	200	HTTP				1,213...
39	200	HTTP				72,785
						588

Malvertising servers used in this attack, and corresponding activities in the last 24 hours (UTC)

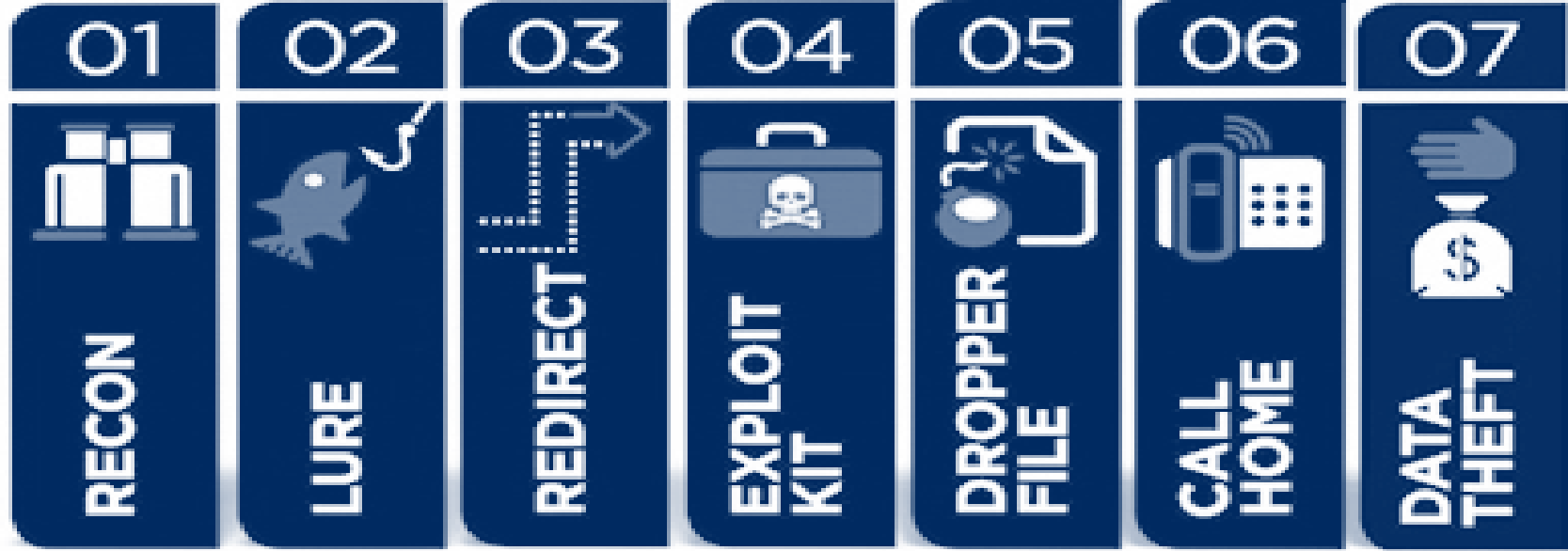


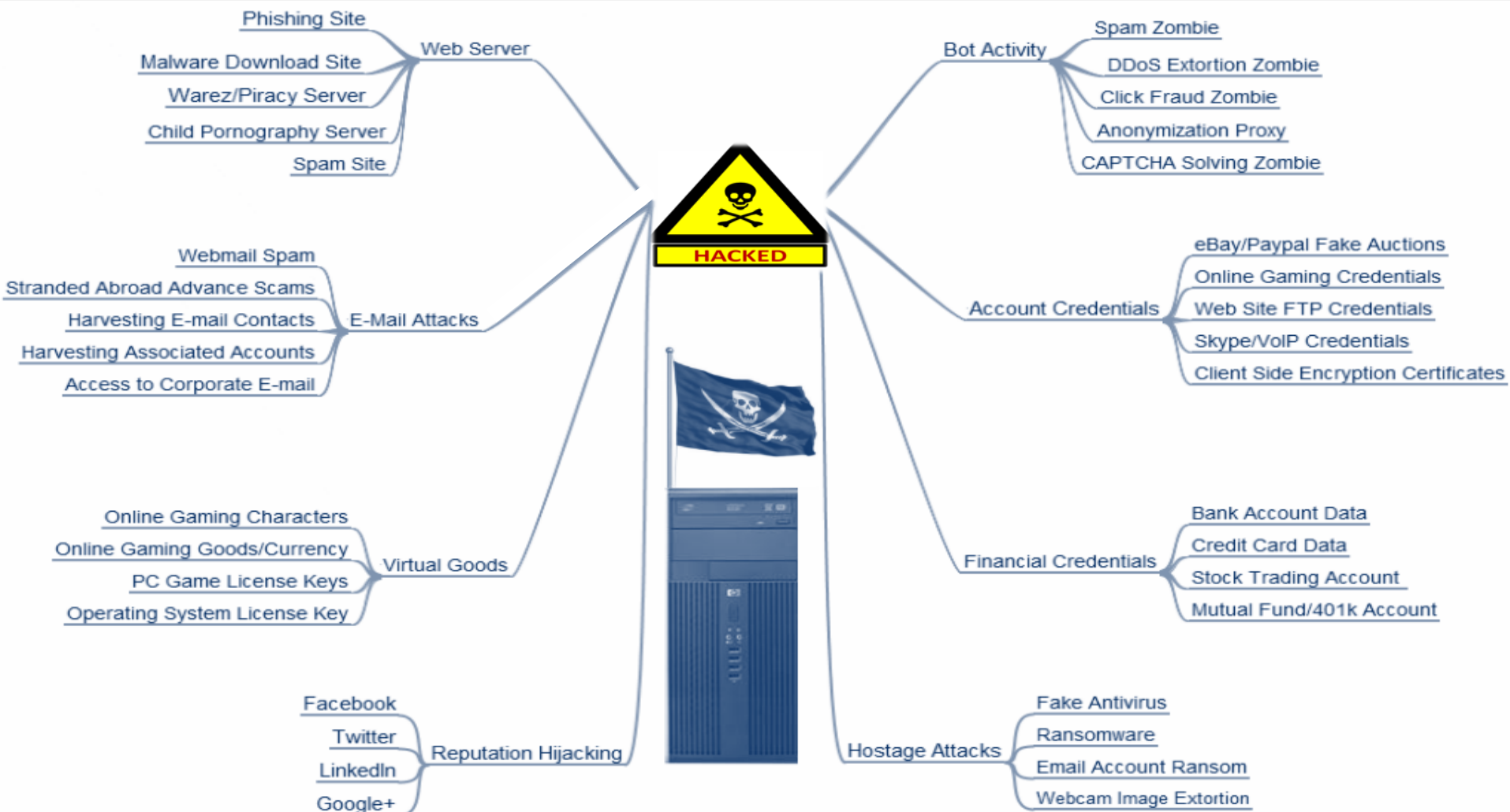
Angler Infections



Figure 2. Geographic distribution of users affected by Angler

Cyber Kill Chain






Enterprise-wide CyberRisk Trends




Our clients are seeking security solutions that are business driven processes to manage information risk and protect the value of their brand.

What's gaining significance...

- 
- ✓ Regulatory requirements: increasing number and complexity, often overlapping and/or competing
 - ✓ IT and internet are integrated into all major business processes introducing risk from every angle
 - ✓ New technologies, geographies and workforce trends pose new cybersecurity threat vectors
 - ✓ People being specifically targeted and lower-tech risks to security steadily increasing
 - ✓ Public communication and reporting of security breaches – more scrutiny to cyber risks

What's losing significance...

- 
- ✓ Reliance on 'penetration testing' as the metric to measure security
 - ✓ Trust of promoting technical resources to build CyberRisk strategy
 - ✓ Belief that security is only a technical problem is waning.
Responsibilities moving to the boardroom.



CyberRisk Solutions Overview

Who is CyberRisk Solutions?



CyberRisk Solutions, LLC provides Enterprise Risk Management strategic consulting, project outsourcing, staffing and managed solutions to reduce the risk of cyber loss and increase operational efficiency for the SMB market across financial services, healthcare, energy and other verticals.

"We're helping define emerging cybersecurity requirements and regulations through our leadership positions within public and private industry standards advisory committees"

"We have the security operations and delivery capabilities required to secure your entire business."



"We start with foundational security program leveraging our deep industry-specific experience to enable critical business processes"





CyberRisk Solutions Services

Enterprise Risk Management (ERM) Solutions Framework



Our solutions follow our business driven process to manage information risk and protect the enterprise to achieve increased shareholder value

Risk Strategy

- ✓ Facilitating the establishment of priorities and resource allocation strategies, oversight, and disclosure in terms of major business risks, regulatory requirements and stakeholder interests

Security Operations

- ✓ Performing daily monitoring and management of security technology to provide deeper insight into threats and provide proactive intelligence

Governance Risk & Compliance

- ✓ Architecting the Policy, Procedures, Processes and Standards for your Risk Management Programs
- ✓ Tending to compliance controls and business value applications of security services

Human Capital

- ✓ Staffing for IT security technology and consulting needs



Risk management for the enterprise for better efficiency, business continuity, regulatory compliance, and limit liability under constantly changing conditions

Virtual Chief Security Officer – V-CSO



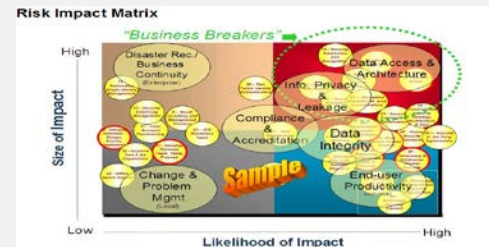
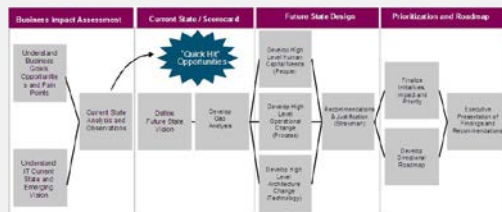
- ✓ A cost effective dedicated Chief Security Officer for the organization and its stakeholders.
- ✓ An executive director and owner of security strategy and risk, linked to organizational objectives.
- ✓ An well-versed executive in all areas of security and able to provide industry best practices.
- ✓ An independent third party to provide direction and strategy for all security decisions.
- ✓ A cost-effective and affordable pricing mechanism that scales with the business.

Enterprise Security Roadmap

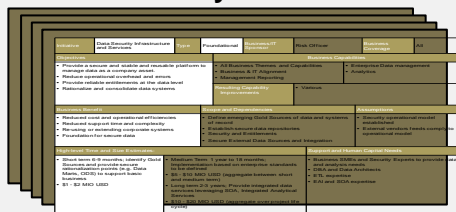


An Assessment you can execute against

Risk
Strategy



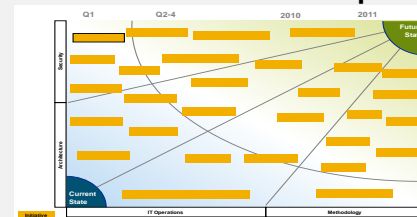
Summary Initiatives



Capability Maturity Model



Future State Road Map



An Enterprise Security Governance & Strategy model executed under a single methodology will drive compliance and sustainability more effectively

Enterprise Security Roadmap



The overall objective of the ESR is to develop a cyber security strategy that aligns with your business direction

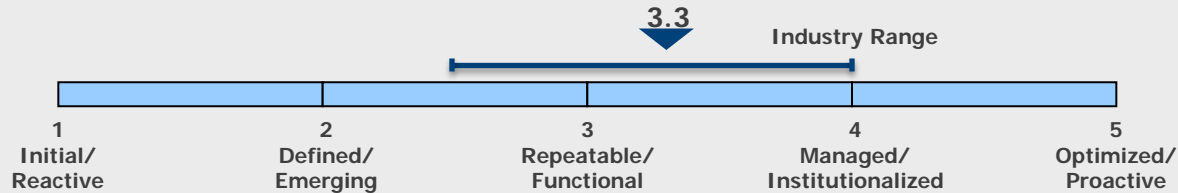
1. Evaluate the current state of information security capabilities and standards using Vaco Risk Solutions Framework, and industry knowledge and experience
2. Define the desired future state vision of information security the client expects to achieve in the next one to three year timeframe
3. Identify the gaps between the current and future states
4. Develop a roadmap plan and set of initiatives to address these gaps

Goal is to provide management with an objective approach to allocating resources

Scoring Methodology, Definitions Example



Example



Scoring Scale & Rating Definitions

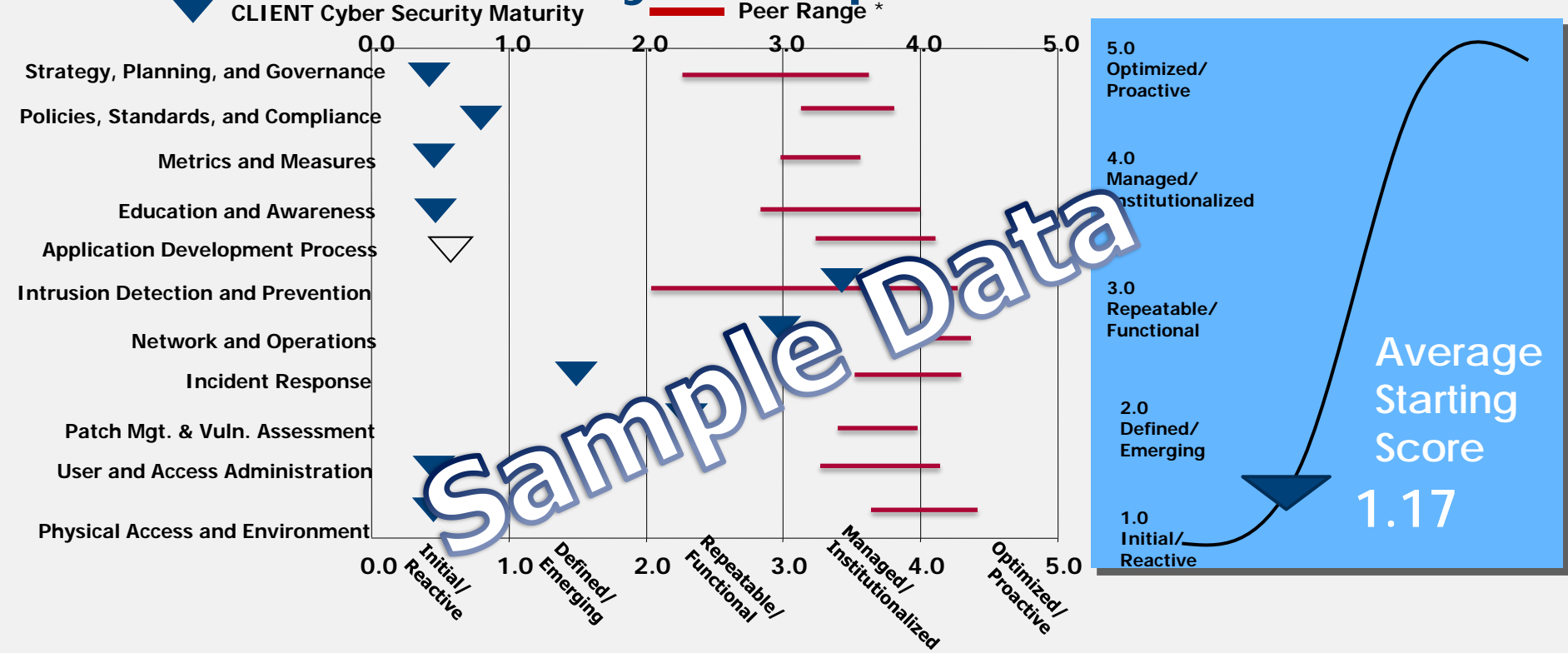
Rating	Description	Process/Policy	Technology
5	Optimized / Proactive	Continuous improvement, ingrained in the organization at all levels	State of the art, integrated systems
4	Managed / Institutionalized	Fully documented and implemented, internalized	Comprehensive solutions, full functionality
3	Repeatable / Functional	Structured and repeatable processes	Partial solutions, limited functionality
2	Defined / Emerging	Informal, non-repeatable	Point solutions, minimal functionality
1	Initial / Reactive	Ad hoc, spontaneous approach	No technology, obsolete

Evaluation Methodology

- Collected factual information
- Collected leadership's perspectives
- Compared process and technology to state-of-the-art
 - ISO2700x
 - Payment Card Industry (PCI-DSS)
 - Industry Practices
- Investigated findings
- Evaluated across multiple dimensions (policy, process, technology)
- Scored by team consensus
- Reviewed by stakeholders



Current State Maturity Standpoint

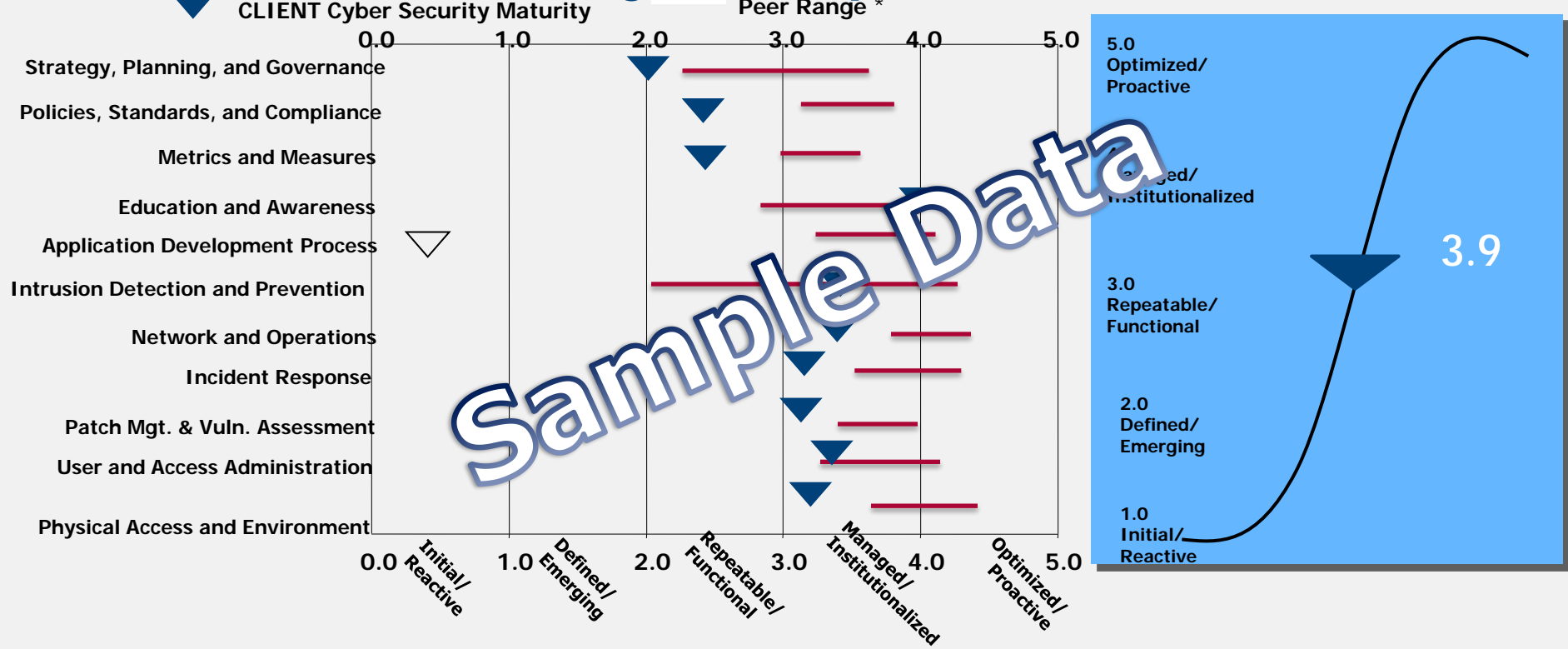


* Norms based on mechanical services which may have higher risk profile due to IP development, national/global presence etc.

Consider cost/benefit of scoring a "5"



Current State Maturity Standpoint



* Norms based on mechanical services which may have higher risk profile due to IP development, national/global presence etc.

Consider cost/benefit of scoring a "5"

Remediation Projects

A. Security Governance and Policies

- A1 - Security Strategy Project
- A2 - Security Organization Project
- A3 - Security Policies & Procedures Project
- A4 - Security Legal Agreements Project
- A5 - External Vulnerability Assessments
- A6 - Bring Your Own Device [BYOD] Strategy
- A7 - eDiscovery
- A8 - Security Dashboard, Metrics & Reporting Process

B. Risk Assessment and Mitigation

- B1 - Risk Assessment Program

C. Human Resources Security and Practices

- C1 - Human Resources Security Project

D. Asset Management and Media Handling

- D1 - Asset Management Project
- D2 - Off-site Storage Project

E. Access Control

- E1 - Design of Access Controls Project

F. Physical / Environmental Security

- F1 - Office Security Project

G. Business Continuity and Disaster Recovery

- G1 - Business Continuity and Disaster Recovery Project

H. Security Awareness and Training

- H1 - Security Training and Certification Project

I. Change Management

- I1 - Change Management

J. Incident Management

- J1 - Incident Response Management Team & Process

K. Network Configuration and Management

- K1 - Network and System Configuration
- K2 - Wireless LAN Architecture and Implementation
- K3 - Automated Patch and Compliance Management
- K4 - Ancillary Systems Vulnerability Management

L. System Monitoring, Logging and Compliance

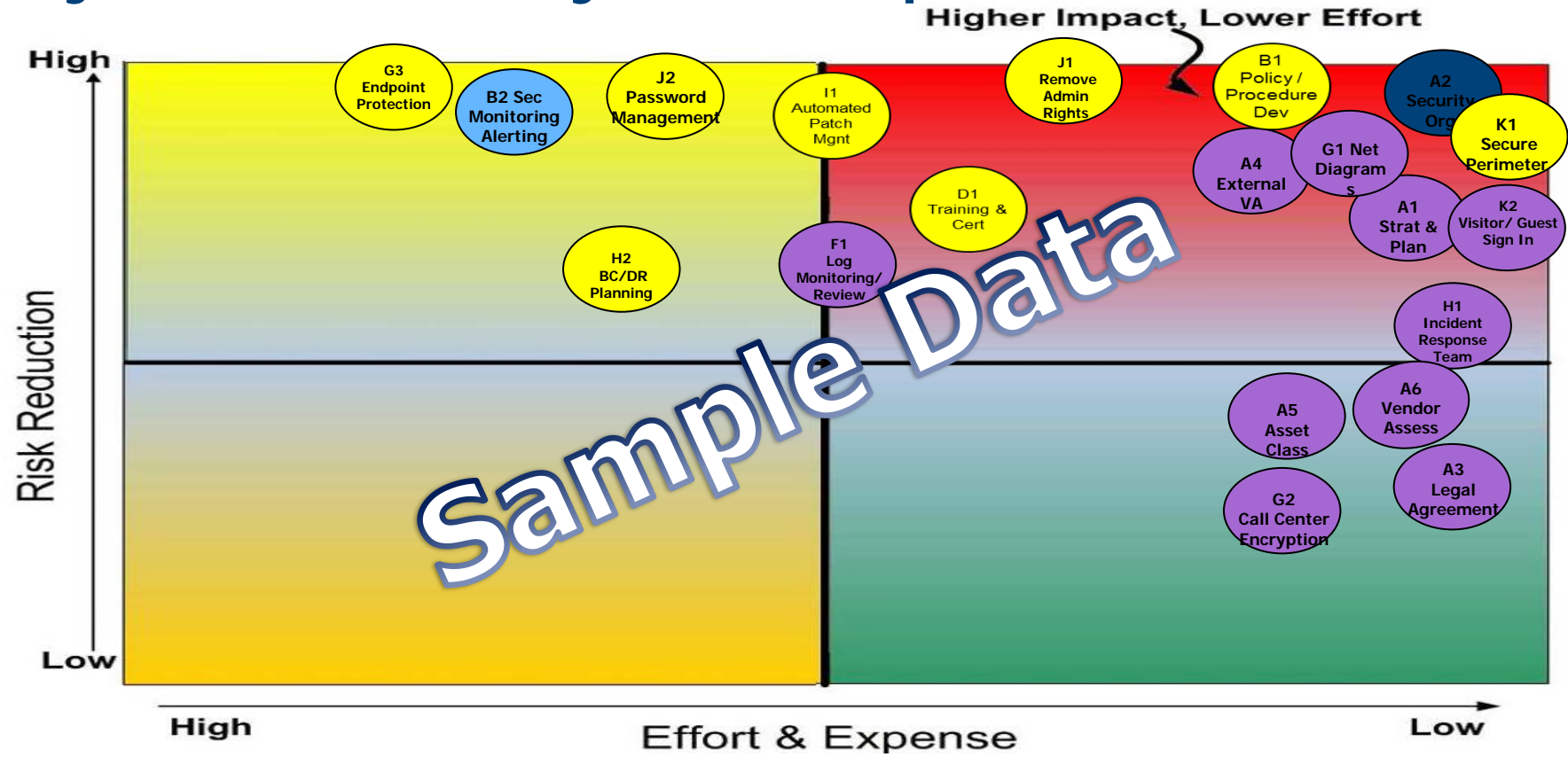
- L1 - Security Monitoring and Review



Addresses Top 4 Risks



CyberRisk Maturity Heat Map



A. Security Governance and Policies

Project A6 – Bring Your Own Device (BYOD) Strategy



Project Overview			
<u>Description</u> Create an Information Security Strategy for BYOD systems that connect to the FirstKey network or are used to access FirstKey data remotely. The strategy will be responsible for: <ul style="list-style-type: none">Defining security requirements – (remote wipe, etc.)Driving necessary changes in security policies and standardsCreating a plan for application support of mobile devices		<u>Success Determination</u> <ul style="list-style-type: none">Policy established with standardsSecurity controls agreed and implementedLegacy applications portal or adapted for mobile devices and rendered via secure gateway (SSL VPN for example)Employees able to use their own devices for and at work	
<u>Benefits</u> <ul style="list-style-type: none">Employees able to use their iPhone, Android phone, or iPad to access FirstKey systems without the need to carry a laptopAppropriate security controls put in place to protect FirstKey dataGreater flexibility for staff and easier access to data		<u>Failure to Act (Consequences)</u> <ul style="list-style-type: none">Lack of policies and standards to address risks. (Personal devices are already being used)Haphazard controls and application supportRisk of information breach or device loss with FirstKey dataOpen to legal action	
3 months (1 month to create and 2 months to implement and refine the approach)			
<ul style="list-style-type: none">Determine key inputsDevelop BYOD strategy & approach		<ul style="list-style-type: none">Pilot the approach and publish results3 months of successful pilot participation	
<ul style="list-style-type: none">None for Strategy		<ul style="list-style-type: none">Application Portal required for BYOD support	
<ul style="list-style-type: none"># of BYOD systems connected	<ul style="list-style-type: none"># of applications adapted		<ul style="list-style-type: none">Standards implemented
<ul style="list-style-type: none">Primarily internal laborExternal guidance for setup and initial implementationParticipation from all major constituents (HR, Legal, Security, etc.)			

A. Security Governance and Policies

Project A6 – Project A6 – Bring Your Own Device (BYOD) Cost



Resource Requirements						
	FY 2015		FY 2016		FY 2017	
	Capital	Expense	Capital	Expense	Capital	Expense
Internal Labor		\$8k		\$4K		\$4K
External Labor		\$25k				
Purchased Services						
Hardware / Software						
Total Costs*		32K		4K		4K
Labor Resources	<ul style="list-style-type: none"> • Business Representation • Legal Representation • Executive Management • Administrative staff • Mobile Strategy Consultant 					
Non-Labor Resources						
	Internal	External	Internal	External	Internal	External
FTE's	100 hours	125 Hours	50 Hours		50 Hours	

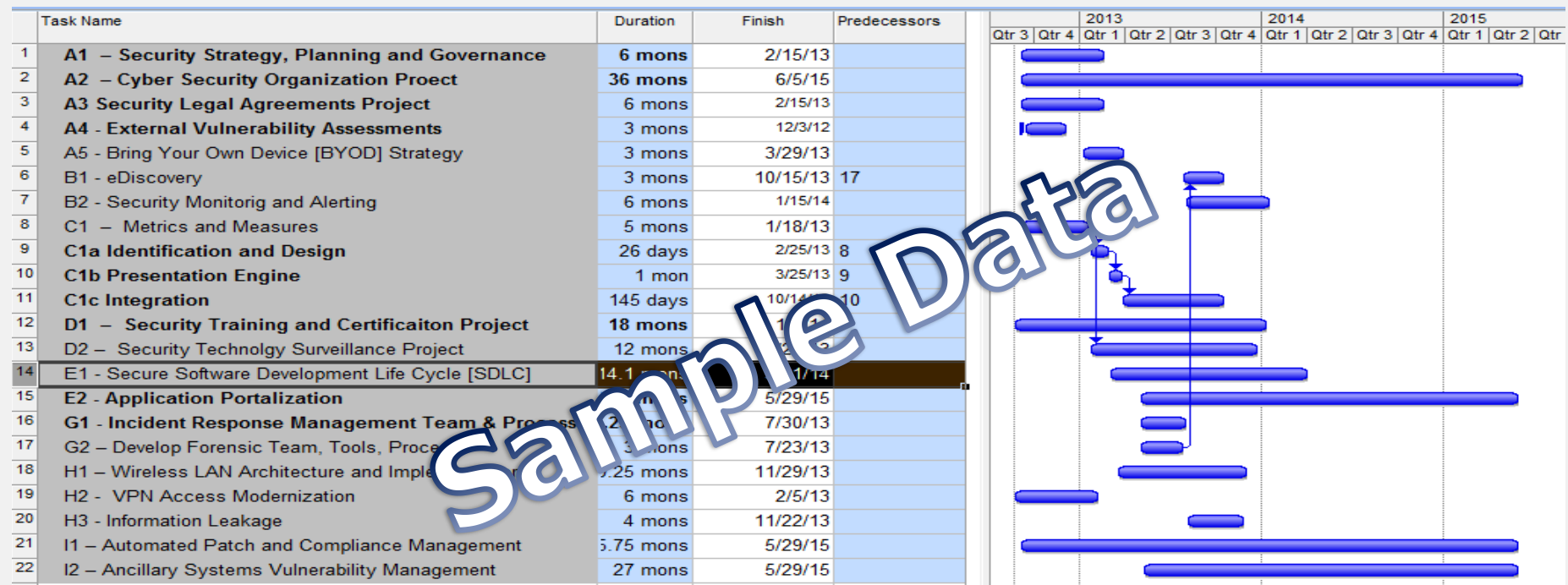
Labor Cost budgeted here for additional internal security FTEs could potentially reduce cost for Roadmap projects or could be absorbed under the individual project budgets.

**** Roll-up of cost for illustration purposes only. Actual labor costs are included as part of each project.**

*** All values shown are ROM costs. Expected project costs are + / - 50% value shown.**



CyberRisk Roadmap



- Project timelines are rough order of magnitude
- Assumptions for start dates were made based on known resources and security project dependencies only. Many factors outside the scope and visibility of this project will determine realistic timeframes.



Unification of all of the compliance targets and program elements

- ✓ Unified Control Framework to build out a GRC program.
- ✓ Business Continuity / Disaster Recovery
- ✓ Incident Response
- ✓ Information Security Policy / Procedures
- ✓ Software Security Assurance

Bringing the program together to be efficient and productive

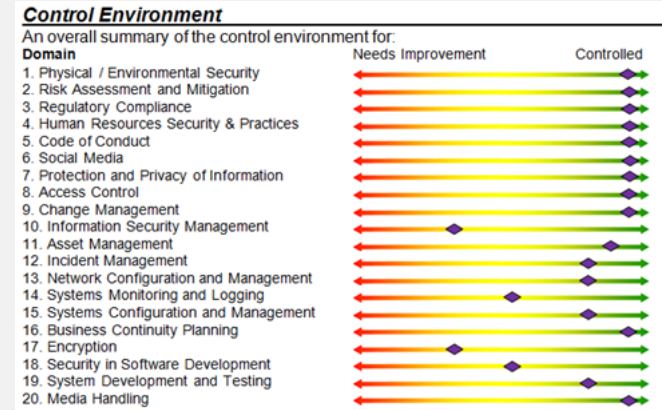
Vendor Risk Management

Third-party Vendor Assessment Methodology (T-VAM)



GRC

- Leveraged in near shore and off shore vendor risk management
- Risk ranking according exposure to the organization
 - ✓ Highly Critical – Tier 1
 - ✓ Important – Tier 2
 - ✓ Incidental – Tier 3
- Reviews 20 controls sets prioritized by the highest vendor risk profiles



Reviews 20 controls sets prioritized by the highest vendor risk profiles



Human Capital

- ✓ Permanent and Temporary Placement
- ✓ Security Technology Staffing
- ✓ Limited Engagement Consulting
- ✓ Security Remediation Staffing
- ✓ Auditing and Reporting

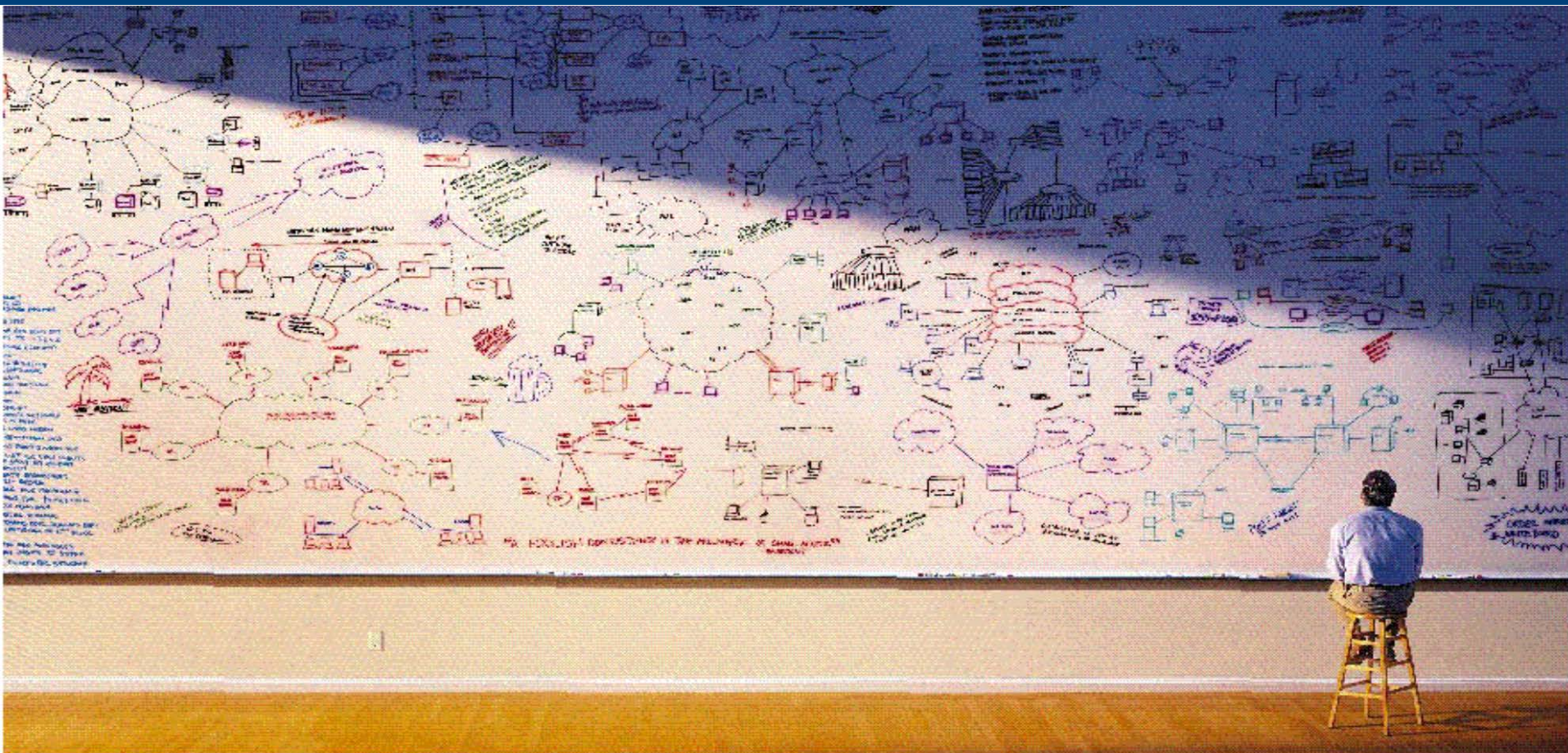


Security Operations

- ✓ 365x24x7 Security Incident and Event Management
- ✓ Network Security Compliance Monitoring and Reporting
- ✓ Correlated event analysis & immediate threat notification
- ✓ Change management to adopt security best practices
- ✓ Compliance & security risk reviews and reporting
- ✓ Easy-to-use, always-on web portal

Outsourcing the day to day operations of your Enterprise Risk Management

Questions



Thank You

Bryant G. Tow, Managing Partner

BTow@CyberRiskSolutionsLLC.com

615.348.RISK (7475)

844.ERM.RISK

(844) 376.7475

