Defense Against Cyber Threats: Strategies and New Developments

September 11, 2013

Prof. Eric Burger MBA, PhD

Director, Georgetown Center for
Secure Communications

Yo Delmar MBA, CMC, CISM, CGEIT

VP of GRC Solutions
MetricStream

MetricStream

Agenda

- A New Set of Risks
- Defense Strategies
- Georgetown Centre for Secure Communications
- Evolving to Cyber Risk Intelligence
- Summary and Call to Action

A New Set of Risks

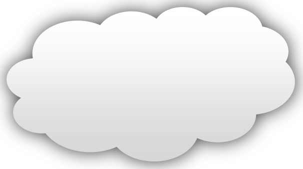
- Cyber Threat Drivers
- Impact of Cyber Threats
- Evolving Threat Landscape
- Who’s Getting Attacked

Cyber Threat Drivers

- Businesses operate across a digital, social, mobile, hyper-extended landscape
- Aggregation of personal and sensitive information creates a target for adversaries - organized crime, nation states and activists
- Disruption Tolerances and Breach Notification windows are shrinking - from hours, to minutes to nano-seconds – reducing the time to detect, respond and report and notify
- Organizations rely on complex global supply chains and service delivery ecosystems – increasing risk across and between many moving parts
- Management seeks Risk Intelligence to drive performance

  → 360 degree view of risks and 'right-sized' mitigation strategies

Big Data

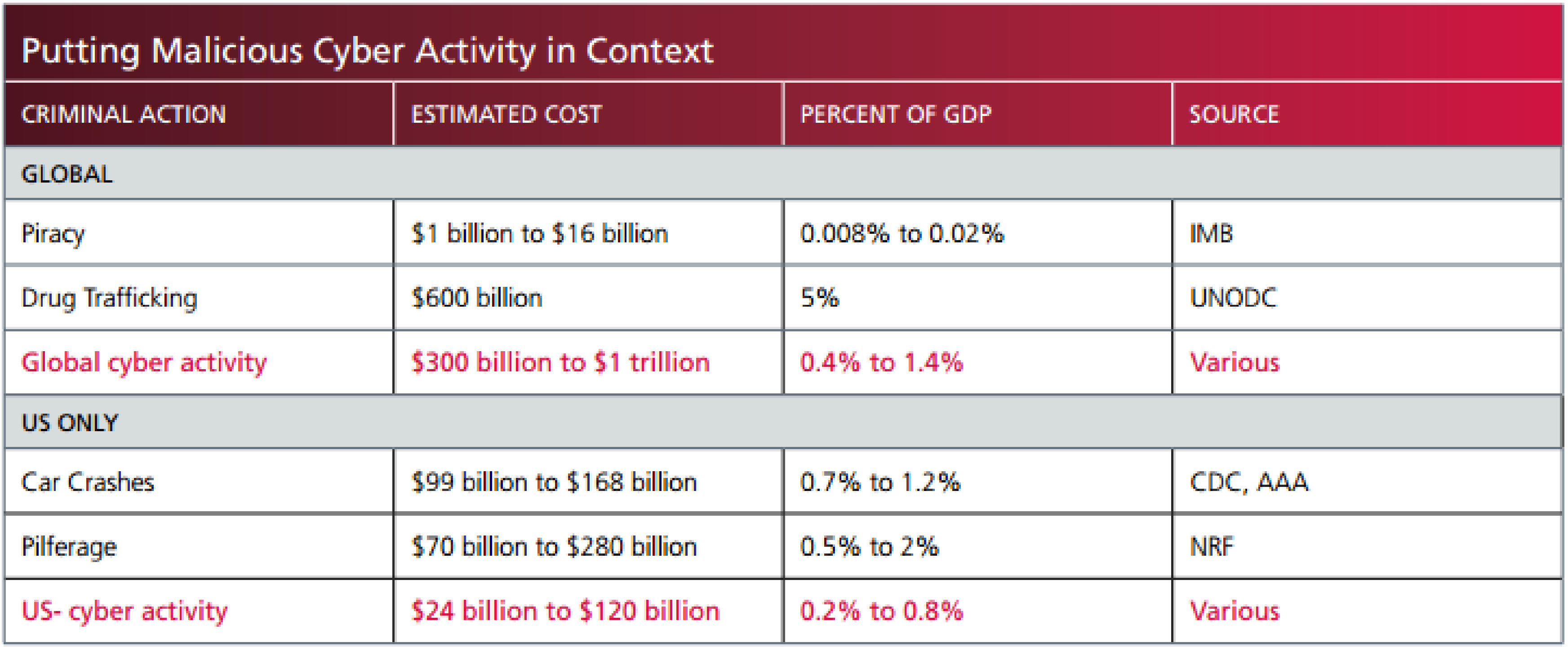


Cloud

Mobile and Social

Critical and Trusted infrastructures

Financial Impact of Cyber Threats - In Context



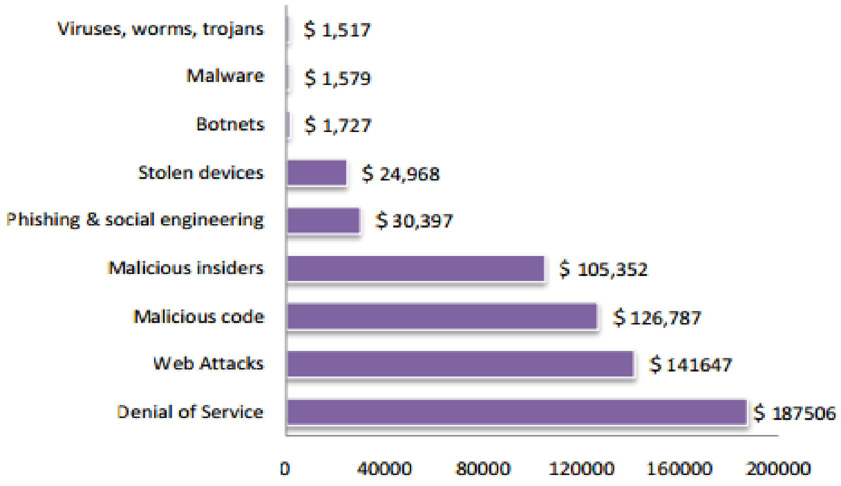
Putting Malicious Cyber Activity in Context

CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Source: McAfee

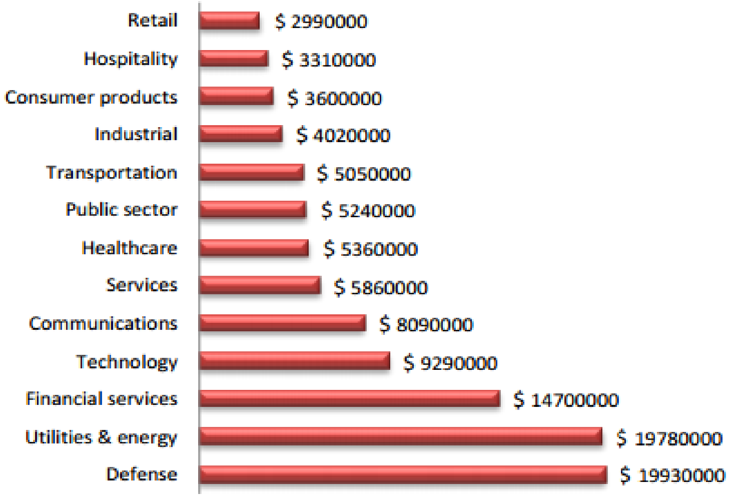
Financial Impact - UN ITU

- It is estimated that overall cost of cybercrime is as much as $1 trillion on a global basis.
- The estimated average cost to an individual US organization was $3.8 million per year in 2010.
- In 2011 the estimated average cost to an individual US organization is $5.9 million per year, with a range from $1.5 million to $36.5 million per organization.
-



Average annual cyber crime cost weighted by the frequency of attack incidents

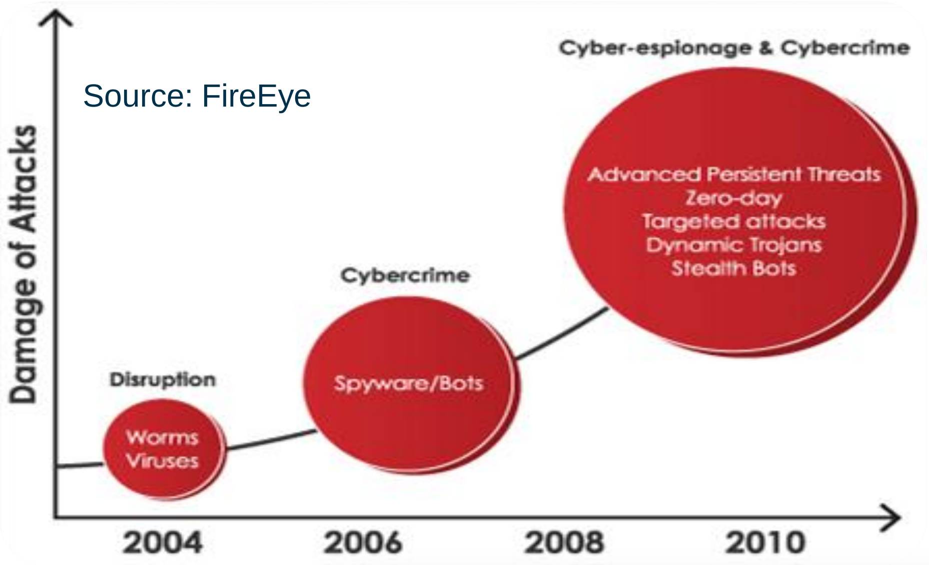
Source: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

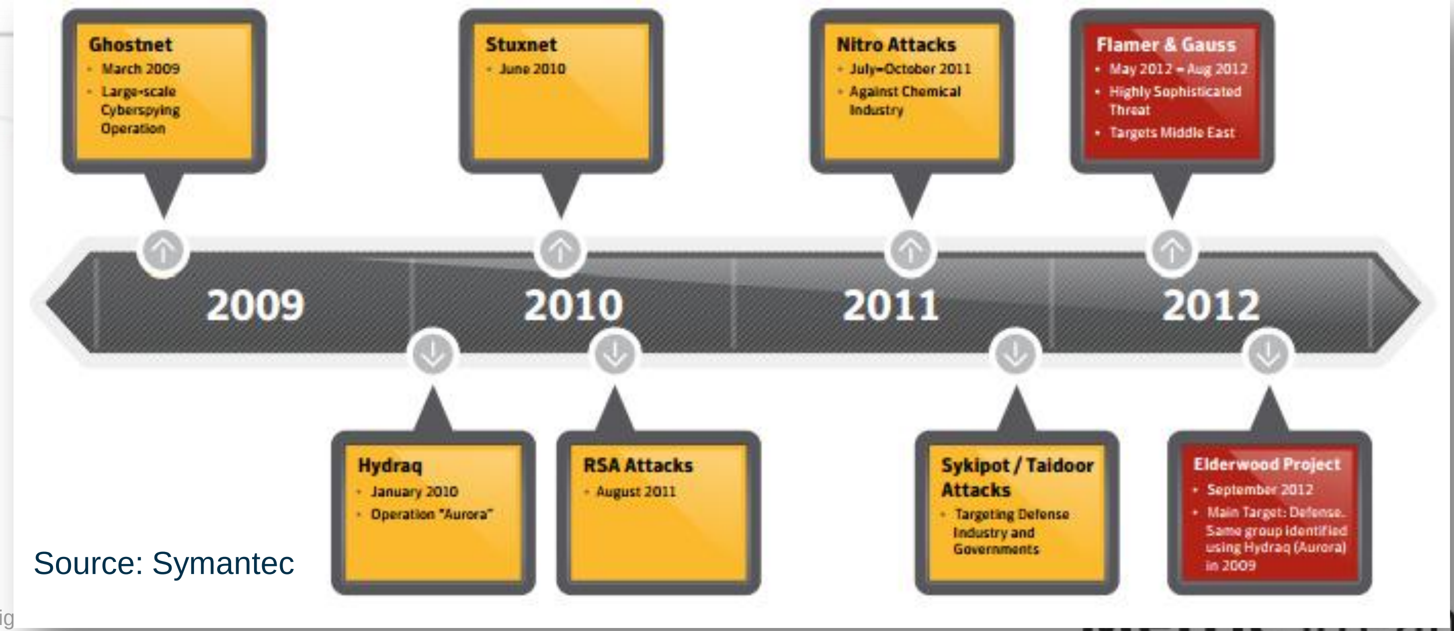


Average annual cost by sector for sample of 50 US organizations for 2011

Source: *http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf*

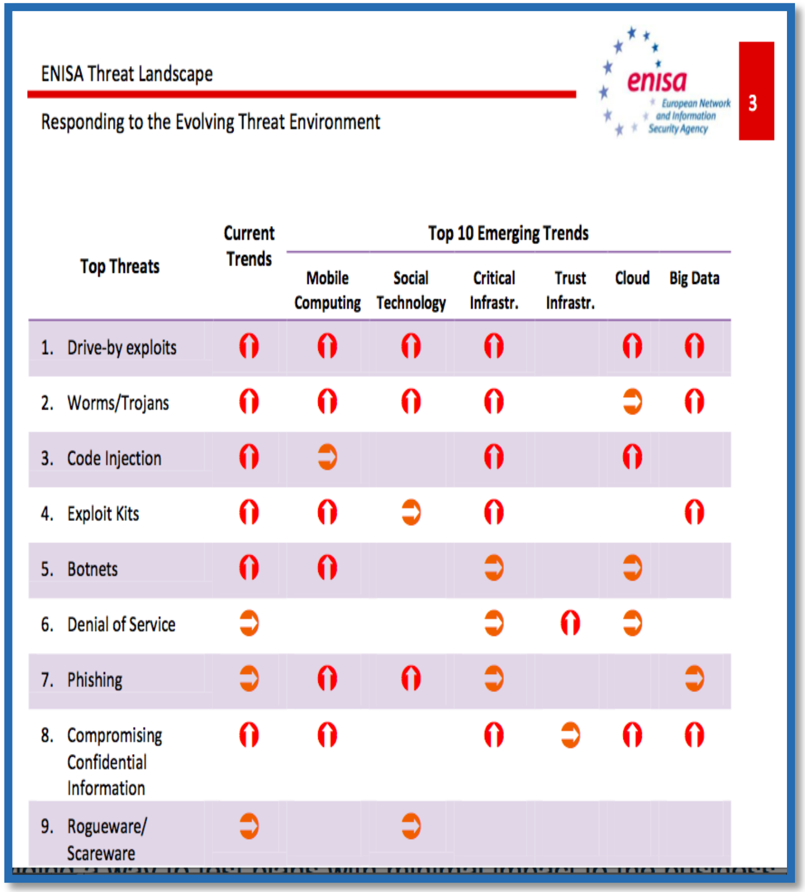
Evolution of Cyber Threats


Source: FireEye


Source: Symantec
Ghostnet
March 2009
Large-scale Cyberspying Operation
Stuxnet
June 2010
Nitro Attacks
July–October 2011
Against Chemical Industry
Flamer & Gauss
May 2012 – Aug 2012
Highly Sophisticated Threat
Targets Middle East
2009
2010
2011
2012
Hydraq
January 2010
Operation "Aurora"
RSA Attacks
August 2011
Sykipot / Taidoor Attacks
Targeting Defense Industry and Governments
Elderwood Project
September 2012
Main Target: Defense. Same group identified using Hydraq (Aurora) in 2009

Evolving Threat Landscape

- Top 5 Threats
  - Drive by exploits
  - Worms/Trojans
  - Code Injections
  - Botnets
  - DDOS
- Emerging Threats
  - Mobile Computing
  - Social Technology
  - Critical Infrastructures
  - Trust Infrastructure
  - Cloud Computing
  - Big Data
- "Notorious Nine" by Cloud Security Alliance
  - Data Breaches
  - Data Loss
  - Account Hijacking
  - Insecure APIs
  - Denial of Service
  - Malicious Insiders
  - Abuse and Nefarious Use
  - Insufficient Due Diligence
  - Shared Technology Issues



ENISA Threat Landscape

Responding to the Evolving Threat Environment

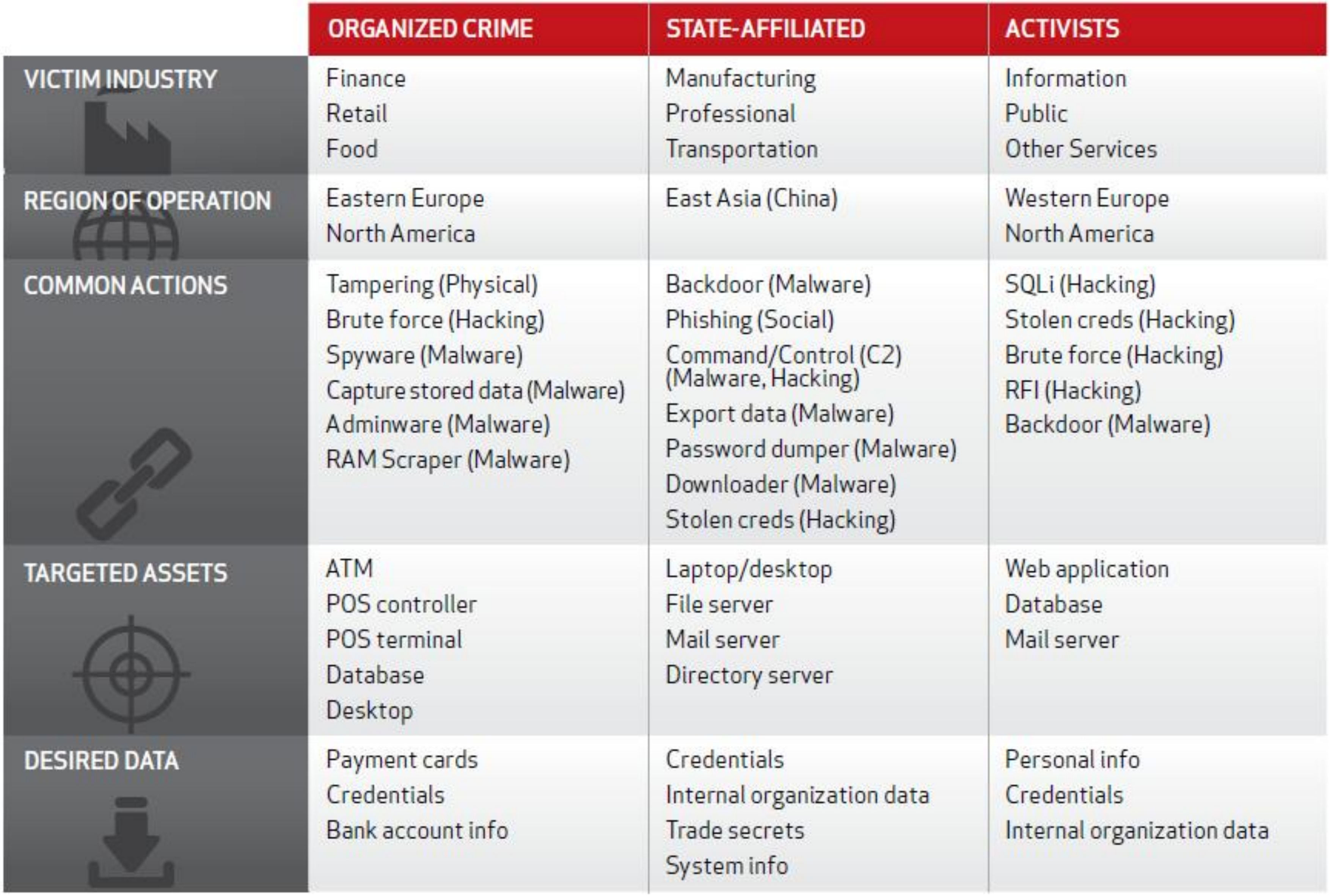
enisa
European Network and Information Security Agency

3

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				

ENISA Threat Landscape

Threat Actor Profile – Verizon DBIR 2013



	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

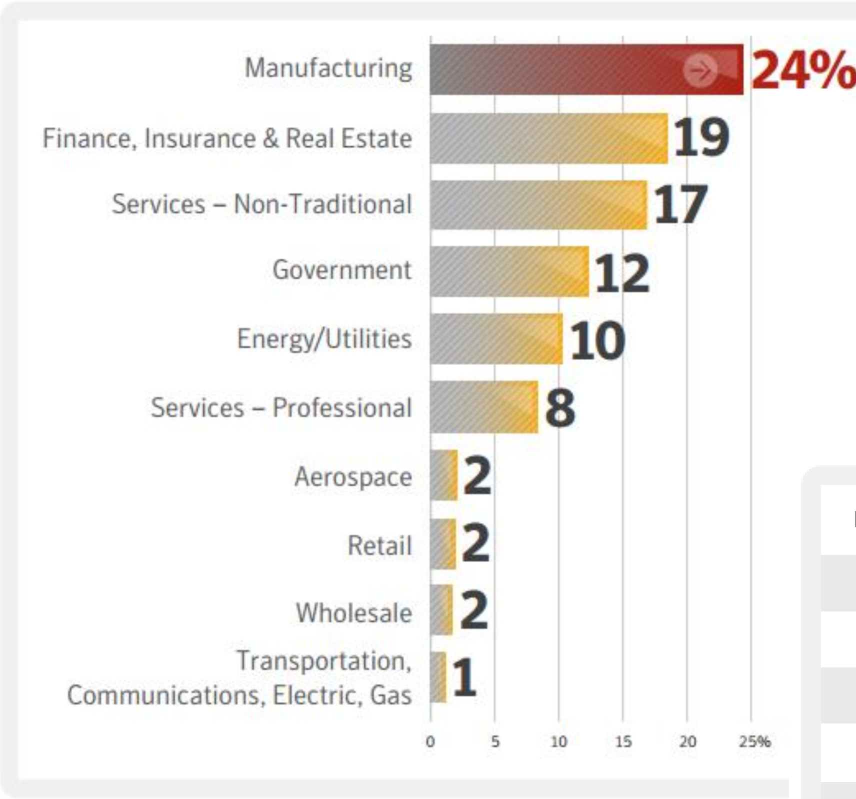
The “A” “P” “T” of APT

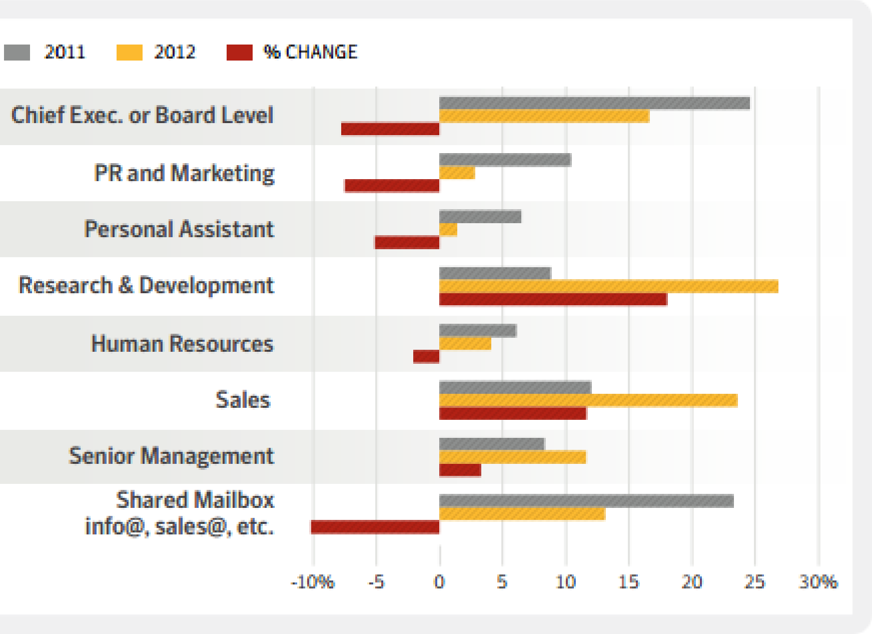
- **A (Advanced)**: This relates to the highly advanced nature of exploitation activity associated with APT-like attacks (zero-day based exploits, sophisticated C2 architectures, target specific AV obfuscation)
- **P (Persistent):** APT attacks persist over a period of time. This is largely due to the long term strategic objectives associated with the operation. Quick gains are sacrificed in pursuit of persistence and stealth, and promise of meeting longer term objectives
- **T (Threat):** This is not a problem that is likely to “go away”. This is an externalized threat typically involving nation state or proxy (nation state) actors

- High-level attack sequence :
  - Reconnaissance
  - Selecting the carrier
  - Attaching the payload (RAT/Trojan)
  - Deploying the carrier+payload
  - Exploitation and payload execution
  - C&C
  - Harvesting, escalation and exfiltration

Attacks by Industry Segments & Job Roles

Source: Symantec





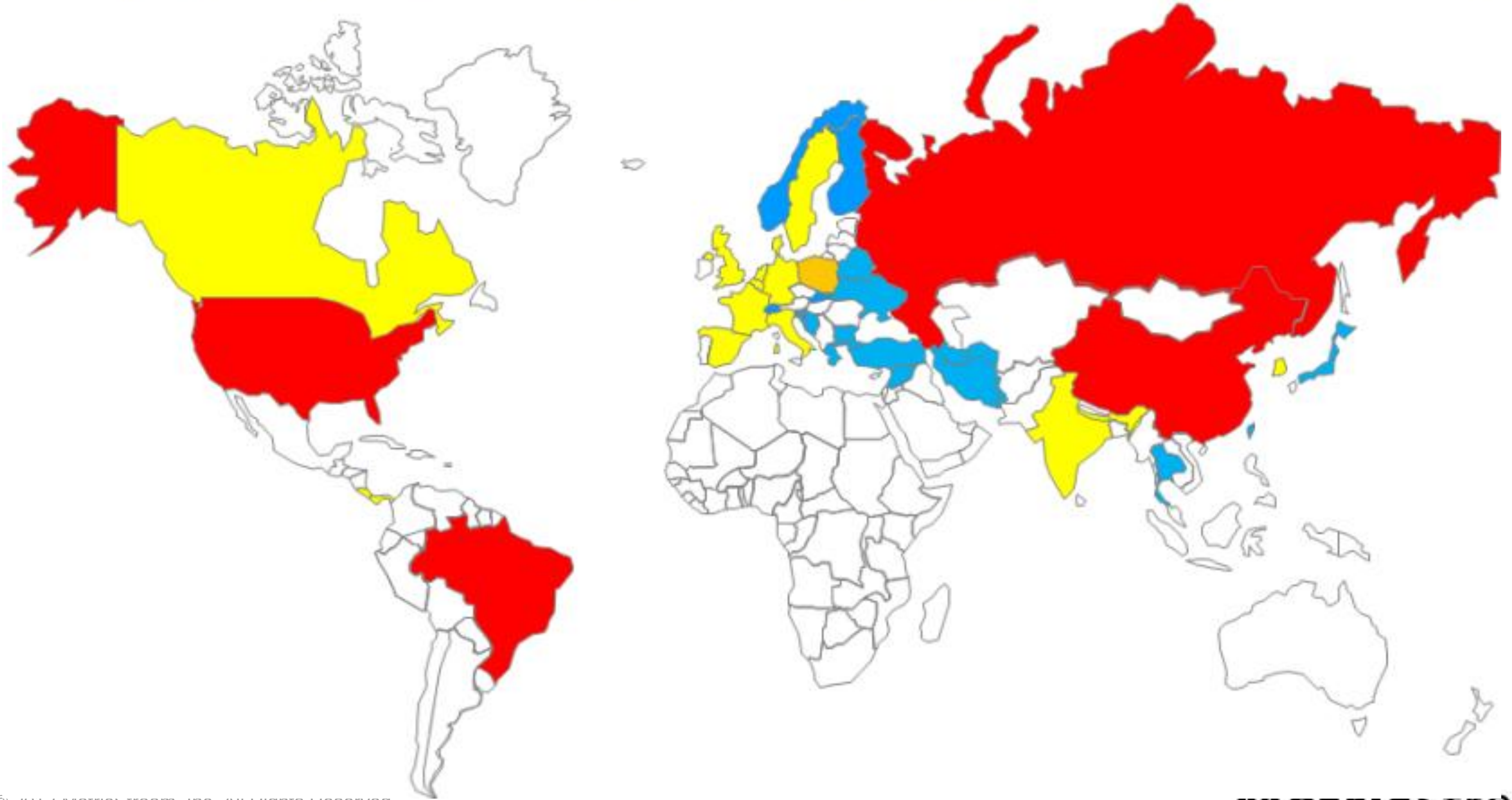
Source: Symantec

Who is Getting Attacked (Source: UN ITU)

Attack Percentage Scale

🟥	High	4.00 % – 25.0%
🟨	Med	1.01 % – 3.99%
🟦	Low	0.11% – 1.00%

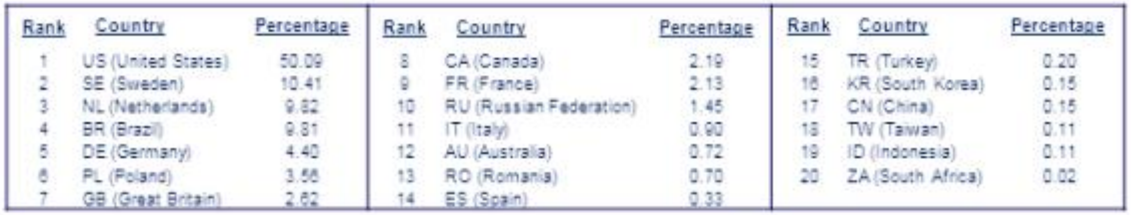
Rank	Country	Percentage	Rank	Country	Percentage	Rank	Country	Percentage
1	United States	24.01	10	South Korea	2.21	19	UAE	0.63
2	China	22.81	11	Panama	2.08	20	Taiwan	0.59
3	Brazil	17.29	12	Japan	1.60	21	Finland	0.56
4	Russia	6.05	13	Sweden	1.51	22	Hungary	0.39
5	Denmark	2.94	14	Spain	1.43	23	Turkey	0.36
6	India	2.77	15	Italy	1.33	24	Norway	0.24
7	United Kingdom	2.73	16	France	1.27	25	Lebanon	0.13
8	Canada	2.72	17	Poland	1.08	26	Luxembourg	0.11
9	Netherlands	2.43	18	Romania	0.7			



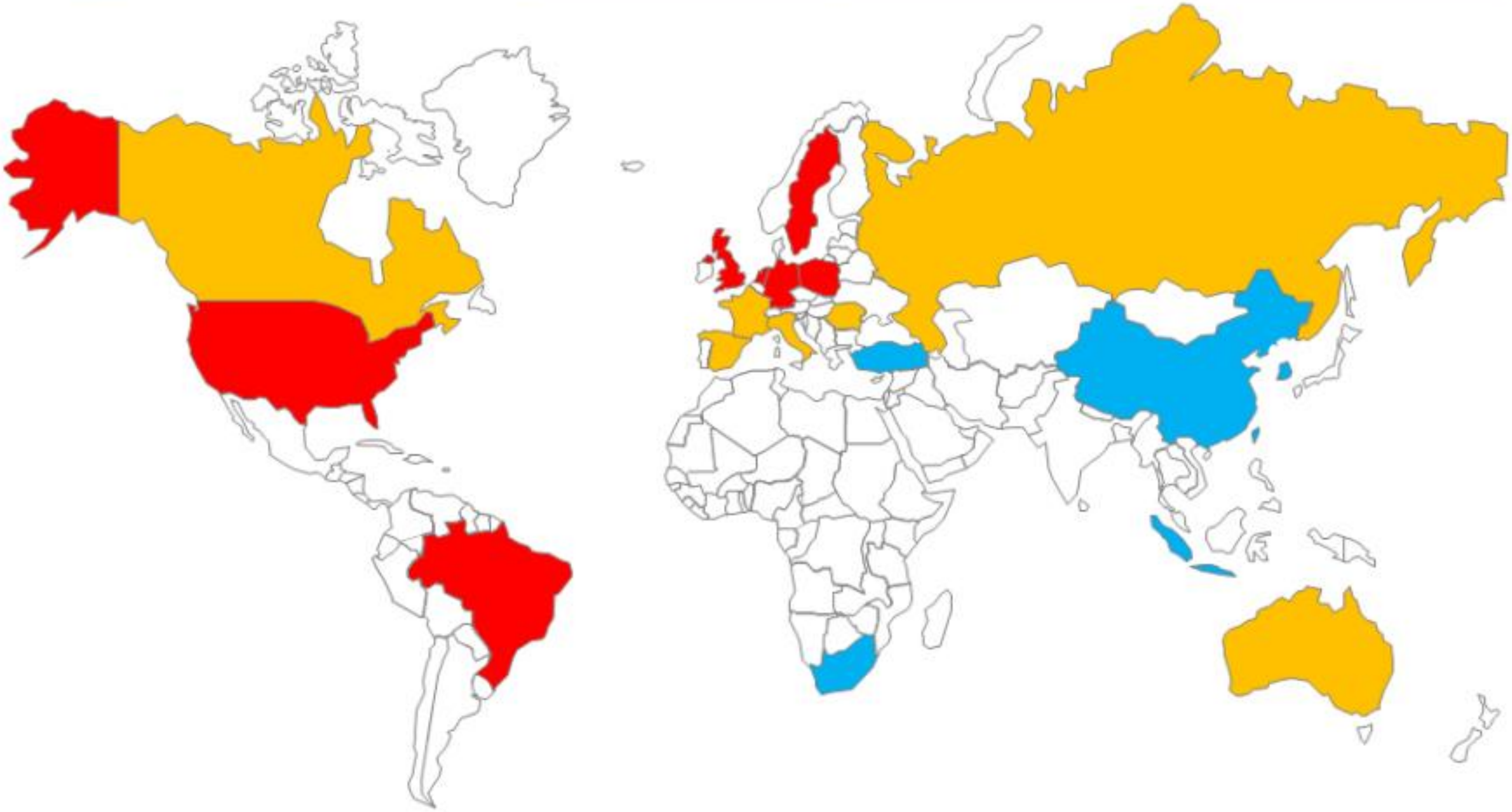
Where Do Attacks Originate (Source: UN ITU)

Attack Percentage Scale

🟥	High	2.62 % – 50.09 %
🟨	Med	0.33 % – 2.19 %
🟦	Low	0.02 % – 0.20 %



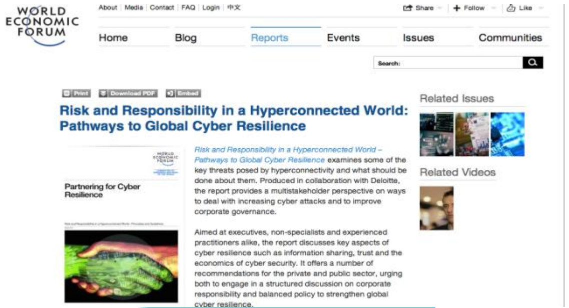
Rank	Country	Percentage	Rank	Country	Percentage	Rank	Country	Percentage
1	US (United States)	50.09	8	CA (Canada)	2.19	15	TR (Turkey)	0.20
2	SE (Sweden)	10.41	9	FR (France)	2.13	16	KR (South Korea)	0.15
3	NL (Netherlands)	9.82	10	RU (Russian Federation)	1.45	17	CN (China)	0.15
4	BR (Brazil)	9.81	11	IT (Italy)	0.90	18	TW (Taiwan)	0.11
5	DE (Germany)	4.40	12	AU (Australia)	0.72	19	ID (Indonesia)	0.11
6	PL (Poland)	3.56	13	RO (Romania)	0.70	20	ZA (South Africa)	0.02
7	GB (Great Britain)	2.62	14	ES (Spain)	0.33			



Defense Strategies

- WEF Cyber Maturity Model
- WEF Cyber Risk Framework
- Modeling the Attack – the Kill Chain
- Defense Strategies

World Economic Forum (WEF) Cyber Maturity Model

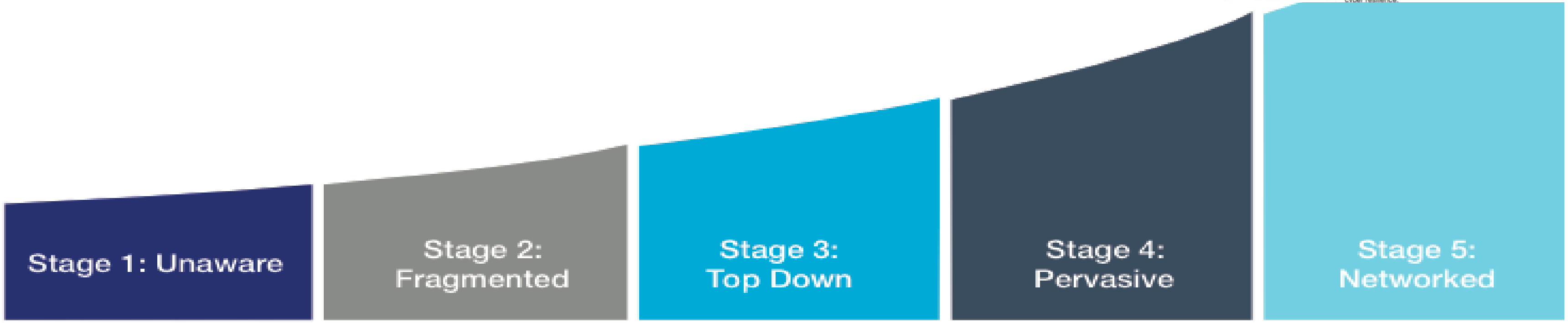


Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience

Risk and Responsibility in a Hyperconnected World – Pathways to Global Cyber Resilience examines some of the key threats posed by hyperconnectivity and what should be done about them. Produced in collaboration with Deloitte, the report provides a multistakeholder perspective on ways to deal with increasing cyber attacks and to improve corporate governance.

Aimed at executives, non-specialists and experienced practitioners alike, the report discusses key aspects of cyber resilience such as information sharing, trust and the economics of cyber security. It offers a number of recommendations for the private and public sector, urging both to engage in a structured discussion on corporate responsibility and balanced policy to strengthen global cyber resilience.

Maturity Model



The organization sees cyber risk as largely irrelevant, and cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness.

The organization recognizes hyperconnectivity as a potential source of risk, and has limited insight in its cyber risk management practices. The organization has a siloed approach to cyber risk, with fragmented and incidental reporting.

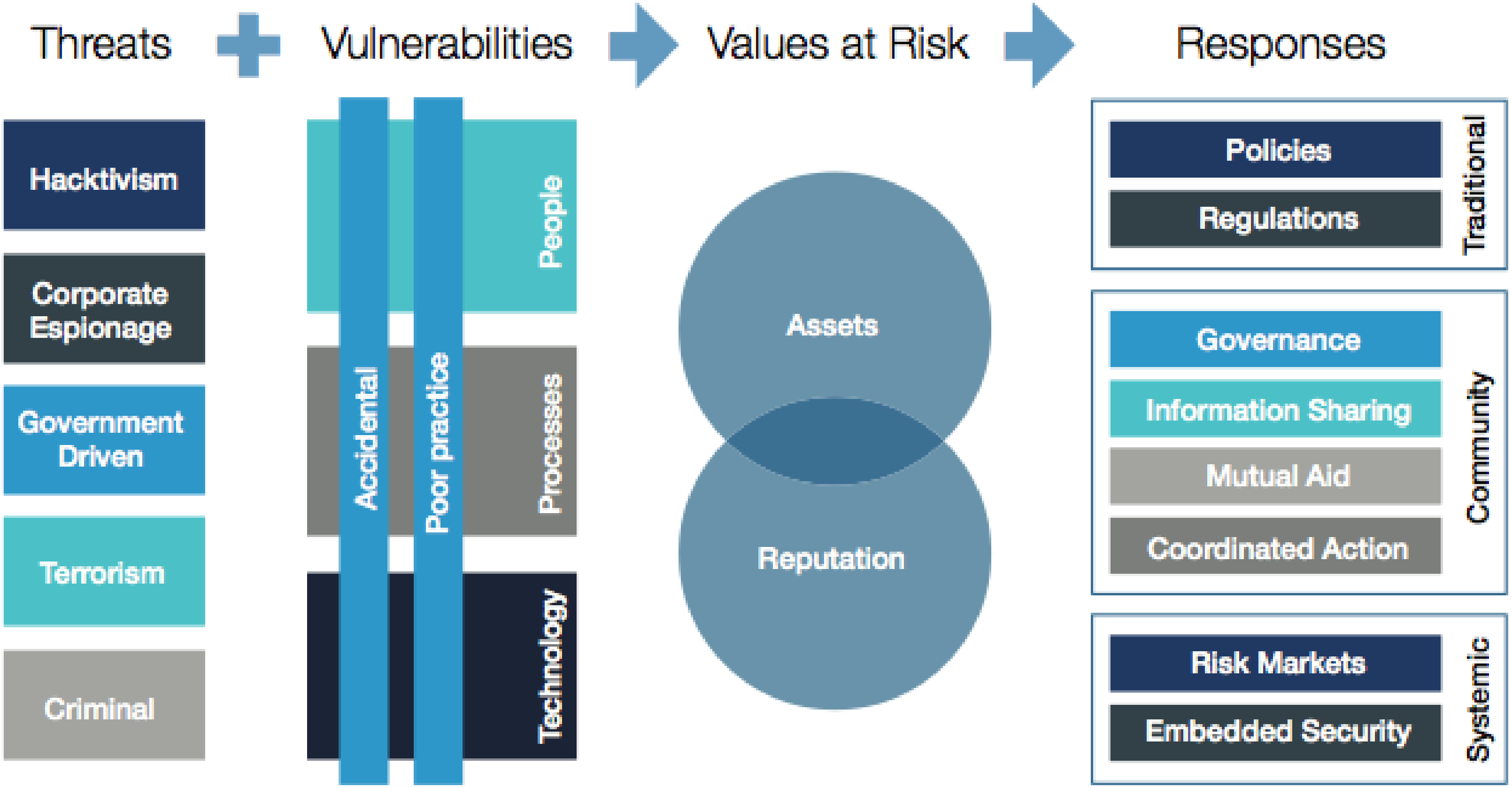
The Chief Executive Officer has set the tone for cyber risk management, has initiated a top-down threat-risk-response program but does not view cyber risk management as a competitive advantage.

The organization's leadership takes full ownership of cyber risk management, has developed policies and frameworks, and has defined responsibilities and reporting mechanisms. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

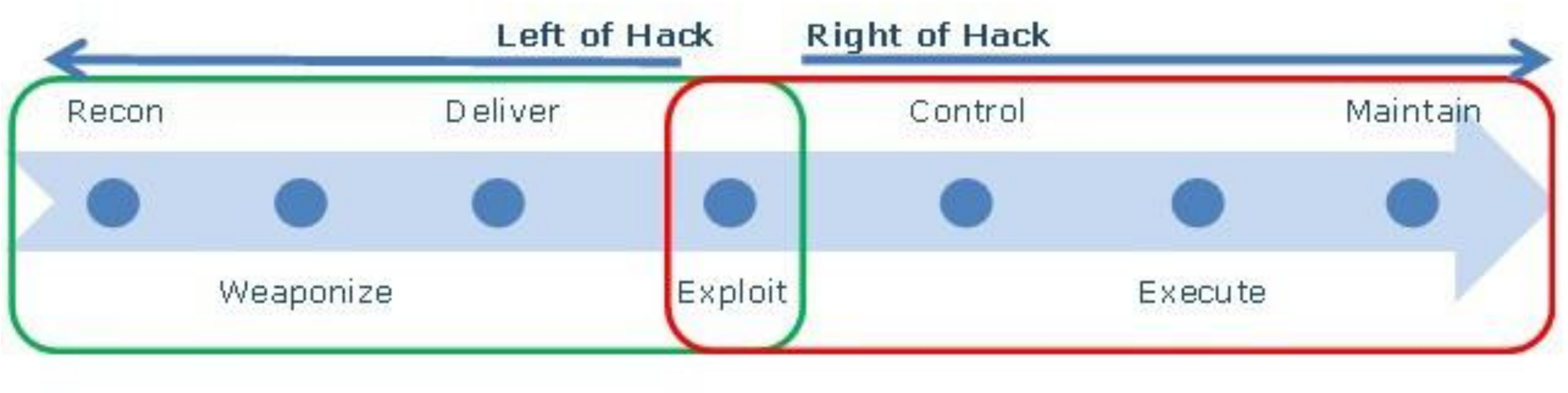
Organizations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day-to-day operations. Its people show exceptional cyberawareness and the organization is an industry leader in managing cyber risk management.

WEF Cyber Risk Framework

Figure 2: Cyber Risk Framework



Modeling the Attack — The Kill Chain

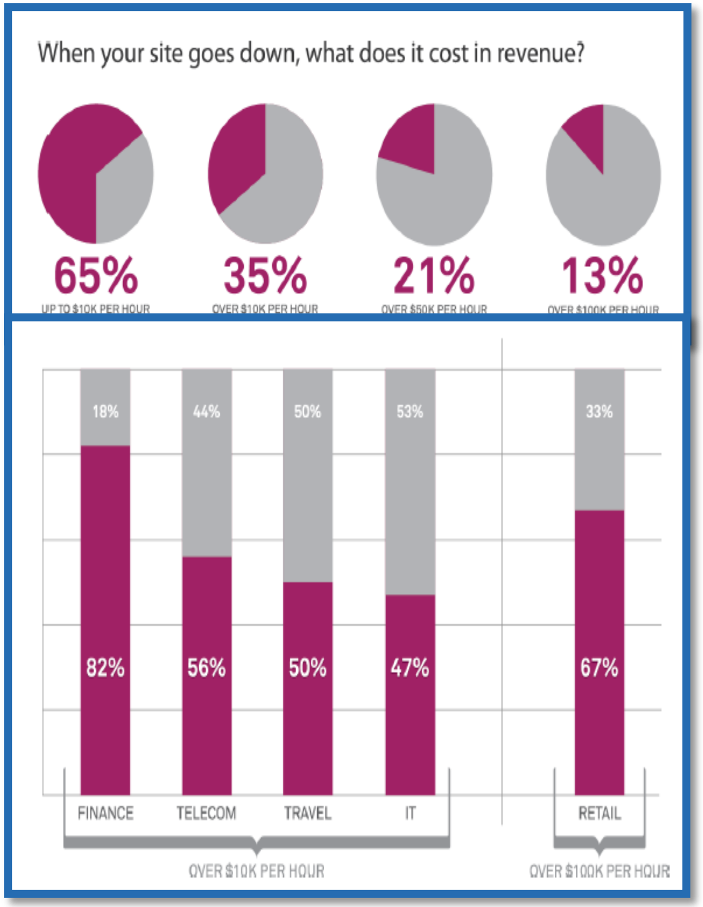


- Just as any thief ‘cases’ the target, attackers reconnoiter, weaponize vectors, deliver, exploit, control, execute and maintain the attack
- The earlier in the kill chain an attack is stopped → the less $ impact and damage

Model developed by Lockheed Martin

Defense Strategy # 1 Know the Impact

- Collect and develop better information and evidence about attack vectors, impact achieved by adversaries, and threat agents
- Develop use cases for threat landscape and map to business objectives, decisions, performance management – become a storyteller
- Agree a level of security required to protect sensitive information and critical assets from cyber threats
- Understand what you are spending on information security now and what you need – build the business case for funding
- Perform a shift in security monitoring, analytics and controls to accommodate emerging threat trends

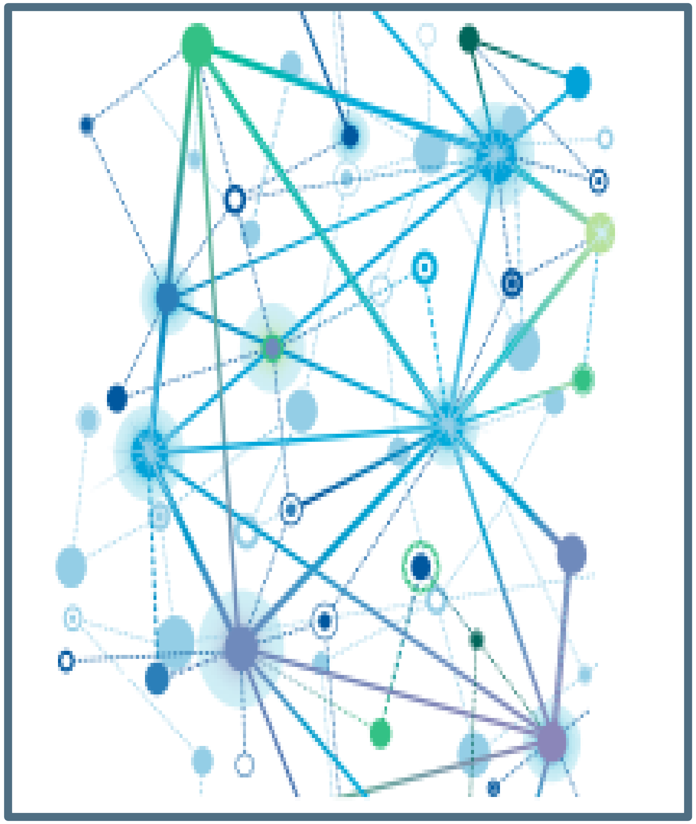


Fund to Cover Impact

Source: Neustar, DDoS Survey 2012

Defense Strategy # 2 Build Security In

- Design your supra-systems *assuming the threat will compromise a subsystem*
- Build in layers of defense and segment your subsystems
- Remember the IPO diagram and monitor the interfaces
- Enforce validation to the specification
- Utilize logging and alerting



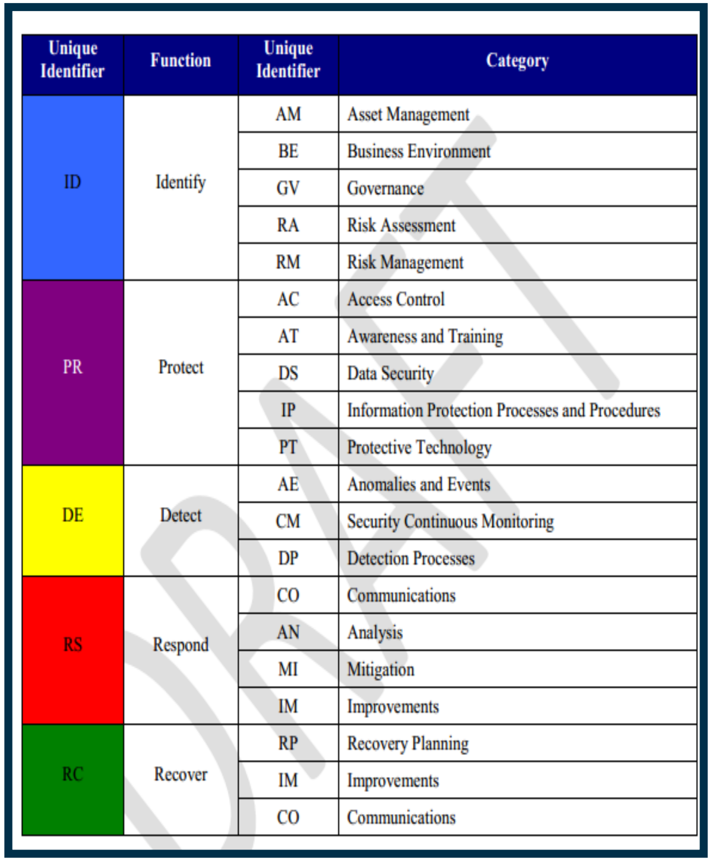
Security By Design

Source: Ernst & Young's Global State of Information Security 2012 Report

MetricStream

Defense Strategy # 3 Continually Assess Risk

- Use industry accepted frameworks and nomenclature (*work in progress*)
- Leverage best-practice frameworks from ISO, NIST, ITU-T and ENISA (*work in progress*)
- Understand your threat environment that is uncontrolled – same vigor as internal information risk assessments
- Audit checklist based approach or “doing security for security’s sake” – not valuable
- Perform detailed and realistic risk assessments and pen tests of critical assets on a near-continuous basis
- Minimize the distance between security controls and capabilities and resources available to the attackers



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

NIST Cyber Security Framework

MetricStream

Defense Strategy # 4 – Monitor and Analyze

- Analyze network traffic
  - Not just viruses any more!
  - Detect abnormally “long” sessions, detect abnormal patterns in bytes/s rates for protocol
  - Detect unexpected / unexplained session management/remote access tools (VNC, RDP)
  - Look for user-agent strings in proxy logs
  - Look for scarce (outlier) records:
    - DNS rejects
    - No route to host
    - Rare web site requests
- More generally, implement a enterprise security incident detection and response program to accomplish the above monitoring objectives as part of a larger comprehensive plan

Security Operations

Defense Strategy # 5 Plan Defensive Moves

- Open Source Analysis
  - Offend: APT will use all the information you give them against you
  - Defend: You can use their analysis to predict their actions
- Attack Phase
  - Offend: Social Engineered Email and Web Site planning
  - Defend: Awareness, Monitoring, Sharing
- Lateral Movement Phase
  - Offend: They will jump to new systems and establish new footholds
  - Defend: Monitor for lateral movement and segregate your networks
- Command & Control and Exfiltration
  - Offend: They will communicate with your systems and take what they want
  - Defend: Block unnecessary outbound traffic, monitor, and share

Moves and Counter Moves

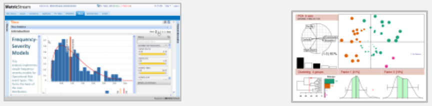
Defense Strategy # 6 Leverage Advanced Analytics

- Define security analytics based on the business process
- Align security metrics and analytics with the enterprise analytics model
- Understand key performance indicators, and map analytics to key risk and control indicators
- Metrics must be meaningful and based on real
- Leverage big data and simulations

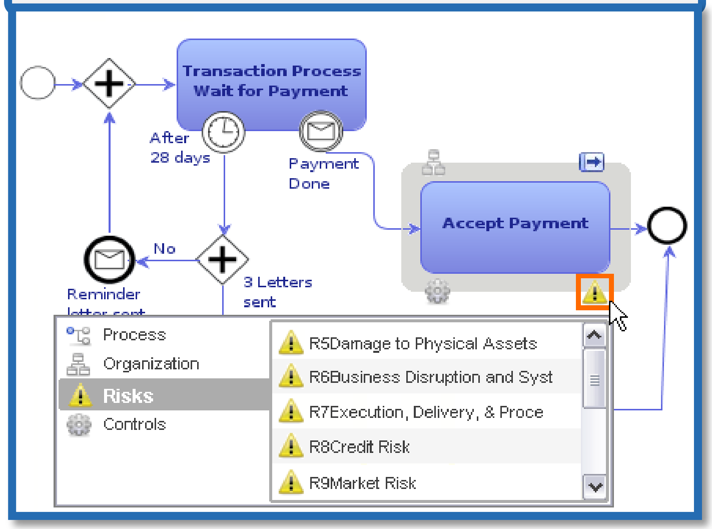
Big Data	**Structured Data**	**Documents/Files**
Hadoop for Email, Social Media, Voice	RDBMS for Application, Security Data	File Systems for Documents and Content

Simulation and Analytics

(R and Other Third-Party Tools)



Statistical Analysis, Simulation Models, Predictive Analytics, etc.



Provide Meaningful Analytics

MetricStream

Defense Strategy # 7 – Share Information

- Submit the malware or suspicious binaries to multi-AV scanning engines such as VirusTotal
- Faster sharing means
  - AV vendors figure it out faster
  - Enterprises learn what is important and is not (yet) important
  - Reduce value of exploit
  - Makes it more expensive to attack
- Not necessarily an admission to being compromised –you just found something abnormal or suspicious and you are being a good (concerned) member of the cyber-community!
- More on sharing later in the Webinar

Share Attribution Info

Defense Strategy # 8 - Collaborate

- Information Sharing and Analysis Centers (ISACs): Sector specific, DHS supported
- Infragard (FBI)
- DIB (USG / defense industry partnership)
- Computer Emergency Response Teams (CERT-CC, US-CERT, CERT-IN, etc.)
- Sector-specific:
  - Transglobal Secure Collaboration Program (TSCP): Large A&D companies and western governments building strategic solutions
  - Network Security Info Exchange (Small international exchange network of Information Security vendors and individuals)
  - Aerospace Industries Association (AIA): 270+ A&D companies sharing ideas
  - Defense Industrial Base (DIB): US Government and Defense Industry partnership
  - NASSCOM (India)
- In cyberspace: Linkedin SIGs, ACM and IEEE SIGs, Information Systems Security Association, etc.

Collaborate in Groups

GEORGETOWN UNIVERSITY
Center for Secure Communications

- Policy
- Technology
- Companies
- Getting Involved

Policy Issues

- It is easy to share information if we are one, homogeneous organization
  - No competitive issues
  - Information shared to operate one’s own networks rarely have legal limits
  - Security technology well-known and understood (e.g., key management)
- What about sharing with
  - Partners
  - Competitors
  - Governments
  - Foreign governments
- What happens when my competition learns of my breach?

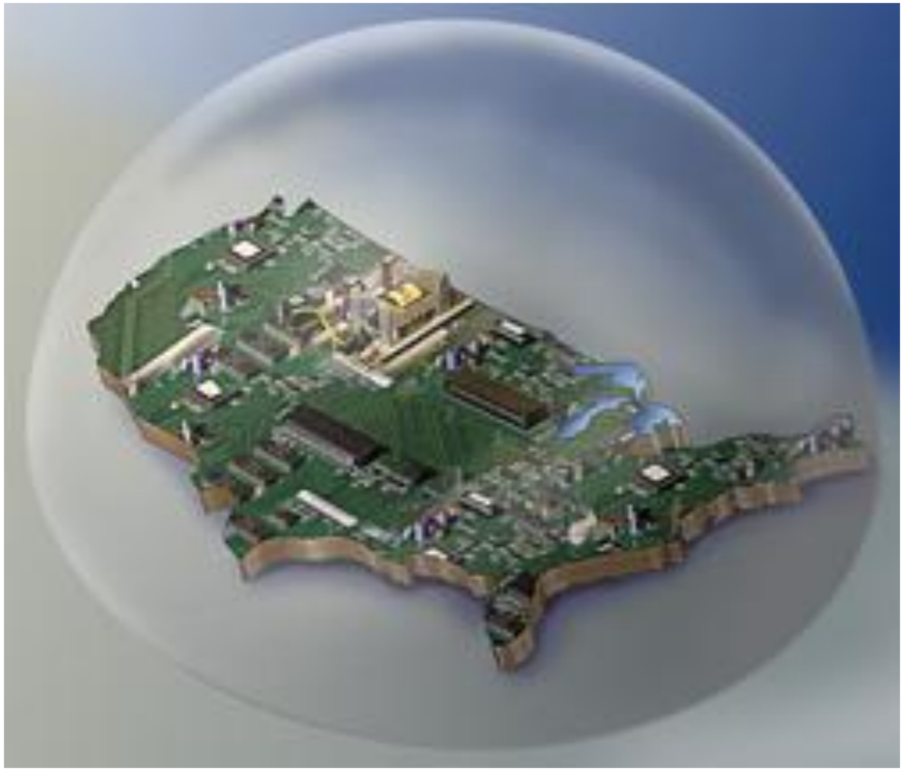


Image credit: Zina Deretsky, NSF

Today’s Solutions

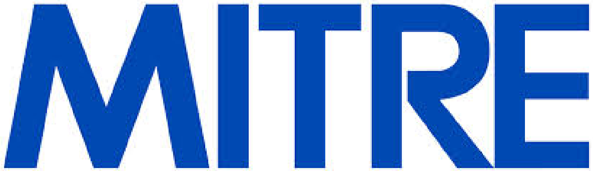
Trusted Networks

We’re All Equals

What the Lawyers Say

No Sharing Allowed

What Technologists Offer



What Companies Need

- **What** can enterprise share with **whom**, **when**?
  - Disclosure laws (PII vs. mandatory disclosure)
  - Different regulations per industry
  - Different laws per country
- Technologies to share at attacker's speed (electronically), not manual speed
  - Reverse cost asymmetry between attackers and defenders

Georgetown Center for Secure Communications

- Addressing the legal, policy, and economic issues
- Informing enterprises, vendors, service providers and governments to create technologies that are
  - Legal to deploy
  - Useful for the customer
  - Economically sensible to use
  - Technologically possible

GEORGETOWN UNIVERSITY

Center for Secure Communications

The Work of the GCSC

What are we delivering?

- Taxonomy of cyber threat intelligence
- Requirements for electronic cyber threat intelligence sharing
- Legal surveys and paths forward
  - US and international
  - B2B and G2B/B2G
- Survey of best sharing practices and experiences
- Economics of sharing
- Technology gap analysis
  - Review of extant technologies
  - Proposals for moving forward

Who is involved?

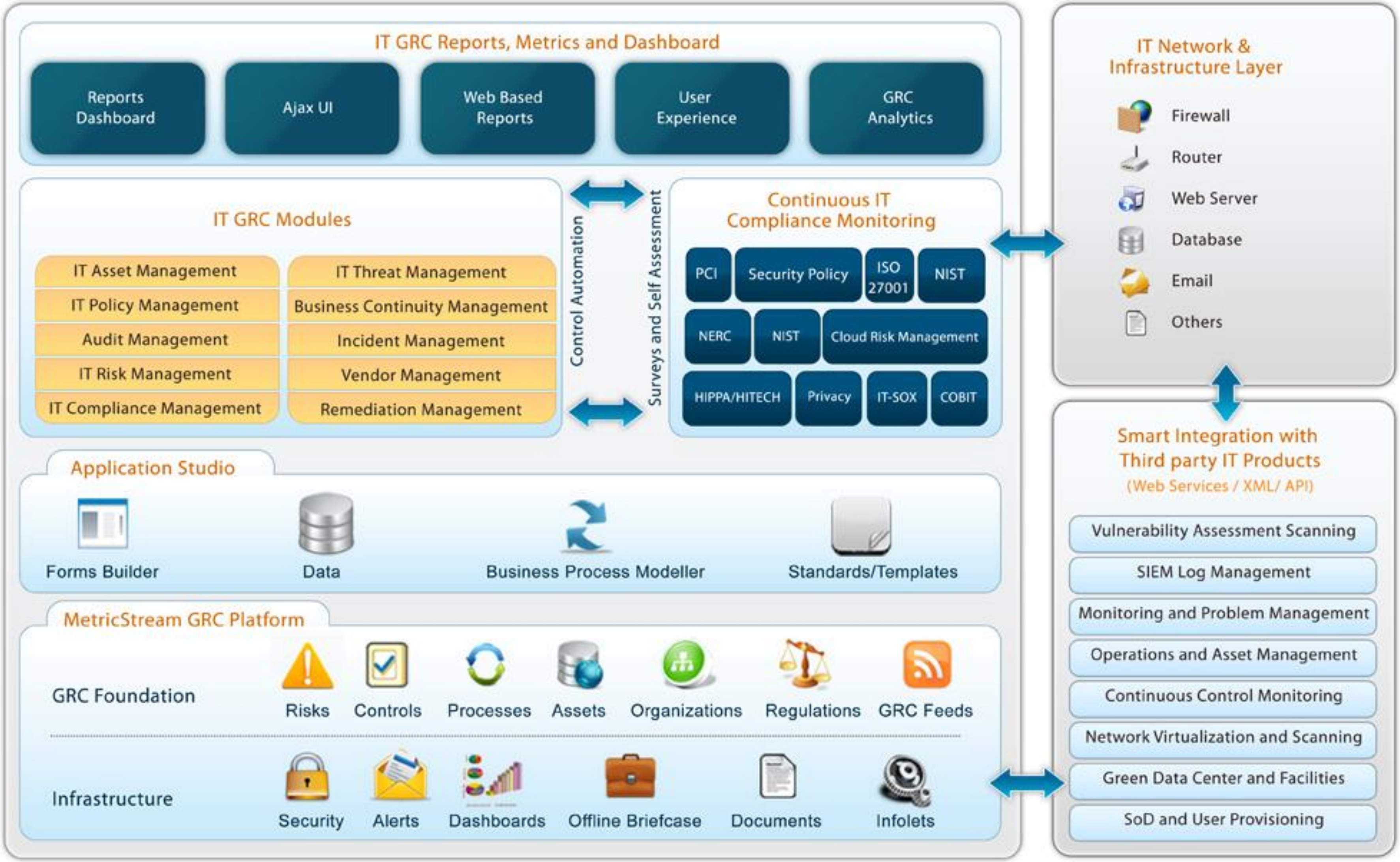
- Private sector enterprises
  - Security vendors
  - Security services providers
  - ISPs
  - Large enterprises
- Public sector enterprises
- Government agencies charged with protecting networks
- Get involved:
  - http://gcsc.georgetown.edu
  - http://s2erc.georgetown.edu/projects/cyberISE/

Evolving to Cyber Risk Intelligence

- Cyber Risk Intelligence Framework
- Big Data Across the Extended Enterprise
- Integrate the View
- Evolve to 360 Degree Risk Intelligence

MetricStream

Cyber Risk Intelligence Framework



IT GRC Reports, Metrics and Dashboard

Reports Dashboard | Ajax UI | Web Based Reports | User Experience | GRC Analytics

IT GRC Modules

IT Asset Management	IT Threat Management
IT Policy Management	Business Continuity Management
Audit Management	Incident Management
IT Risk Management	Vendor Management
IT Compliance Management	Remediation Management

Control Automation

Surveys and Self Assessment

Continuous IT Compliance Monitoring

PCI | Security Policy | ISO 27001 | NIST

NERC | NIST | Cloud Risk Management

HIPPA/HITECH | Privacy | IT-SOX | COBIT

IT Network & Infrastructure Layer

- Firewall
- Router
- Web Server
- Database
- Email
- Others

Application Studio

Forms Builder | Data | Business Process Modeller | Standards/Templates

MetricStream GRC Platform

GRC Foundation: Risks | Controls | Processes | Assets | Organizations | Regulations | GRC Feeds

Infrastructure: Security | Alerts | Dashboards | Offline Briefcase | Documents | Infolets

Smart Integration with Third party IT Products

(Web Services / XML/ API)

- Vulnerability Assessment Scanning
- SIEM Log Management
- Monitoring and Problem Management
- Operations and Asset Management
- Continuous Control Monitoring
- Network Virtualization and Scanning
- Green Data Center and Facilities
- SoD and User Provisioning

‘Big Data’ Across the Enterprise

- Control Tests
- Compliance Issues & Remediation
- Regulatory Compliance
- Regulatory Exam Findings
- Regulatory Filings

- Enterprise Risk Assessments
- Top-Down Risk Perspectives
- Risk Findings & Remediation

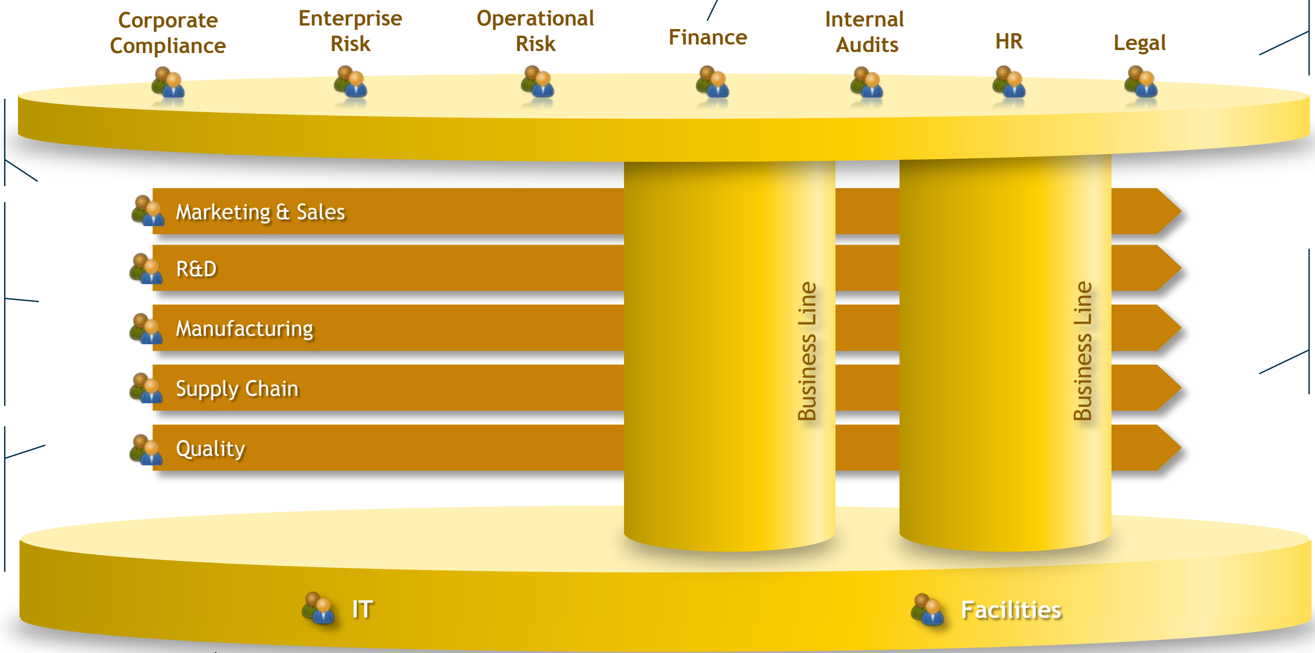
- Losses
- Operational Risk Assessments
- Operational Control Tests
- Federated LOB Risk Perspectives

- General Ledger
- Losses
- Tax Filings
- Financial Transactions

- Independent Risk Perspective
- Control Tests
- Audit Findings & Remediation

- HR Policies
- HR Compliance

- Reputation
- Social & Web monitoring
- Ethics & Fraud Policies
- Legal Matter
- e-Discovery



- Marketing Compliance
- Marketing Activities

- Operating Risks
- Restricted Materials
- Permits
- Permit Filing Calendar
- Non-Compliance Issues

- Non-Conformances
- Complaints
- Part Inspections
- Quality Audits
- CAPAs

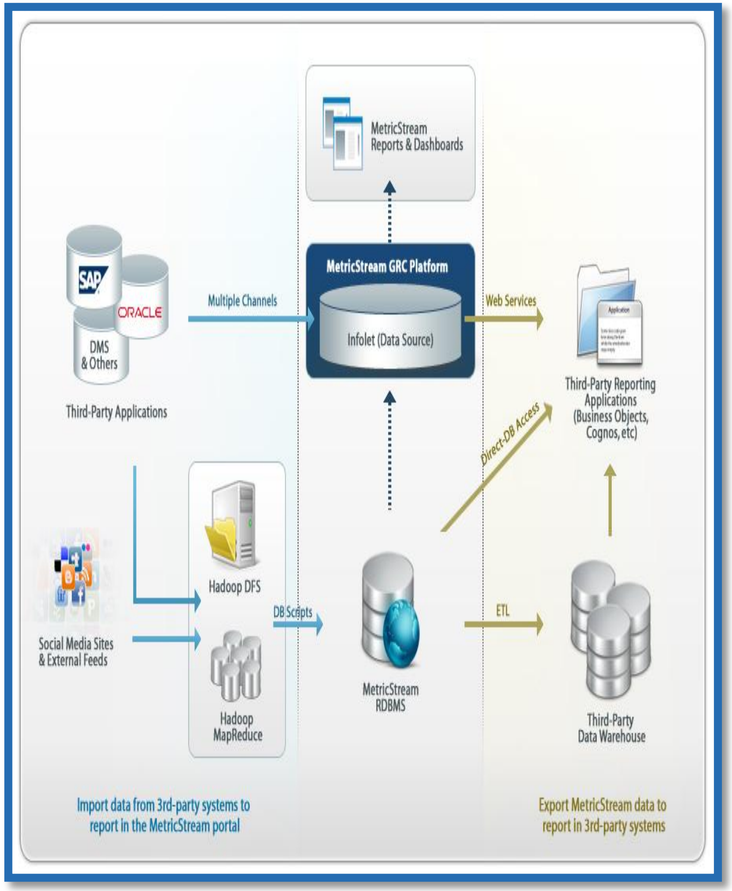
- Supply Chain Risks
- Supplier Scorecards
- Supplier Metrics
- Supply Chain Issues
- Supply Chain Incidents

- Contracts & SLAs
- Regulatory Compliance
- Threats & Vulnerabilities
- Security Incidents
- Configurations
- Roles & Access Rights
- Physical & Virtual Assets

- Health & Safety Compliance
- Emissions Data
- Water & Waste Data
- Facility-Use Policies
- Physical Access

Aggregating Across the Extended Enterprise

- Leverage a common GRC platform, with an asset inventory, and risk and control framework and nomenclature
- Collect and develop better information and evidence about attack vectors, impact achieved by adversaries, and threat agents
- Develop use cases for threat landscapes
- Collect security intelligence that cover incidents in an end-to-end manner
- Perform a shift in security controls to accommodate emerging threat trends
- Question access and think about what you are allowing into your environment

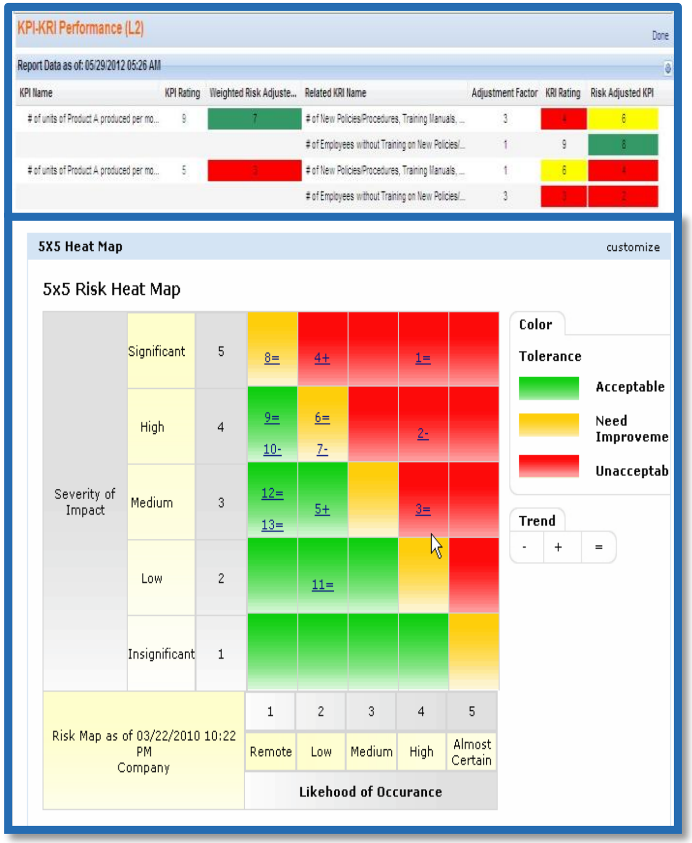

MetricStream Reports & Dashboards
SAP
ORACLE
DMS & Others
Third-Party Applications
Multiple Channels
MetricStream GRC Platform
Infolet (Data Source)
Web Services
Third-Party Reporting Applications (Business Objects, Cognos, etc)
Direct-DB Access
Hadoop DFS
Social Media Sites & External Feeds
DB Scripts
ETL
Hadoop MapReduce
MetricStream RDBMS
Third-Party Data Warehouse
Import data from 3rd-party systems to report in the MetricStream portal
Export MetricStream data to report in 3rd-party systems

Integrate the View

MetricStream

Evolve to 360 Degree Cyber Risk Intelligence

- Streamline risk management - single information model, cross-functional collaboration, multi-dimensional risk assessments
- Analytics: Metrics and Reporting on Cyber risks that support Better Performance
- Linked to and describe risk/exposure in the context of a real business impact
- Map to size, scale and scope of cyber risks in the context of the organization
- Provide options for remediation including people, process and technology costs
- Embed it in the operational fabric of the organization → make it pervasive


KPI-KRI Performance (L2)

Report Data as of: 05/29/2012 05:26 AM

KPI Name	KPI Rating	Weighted Risk Adjuste...	Related KRI Name	Adjustment Factor	KRI Rating	Risk Adjusted KPI
# of units of Product A produced per mo...	9	7	# of New Policies/Procedures, Training Manuals, ...	3	4	6
			# of Employees without Training on New Policies/...	1	9	8
# of units of Product A produced per mo...	5	3	# of New Policies/Procedures, Training Manuals, ...	1	6	4
			# of Employees without Training on New Policies/...	3	3	2

5X5 Heat Map

5x5 Risk Heat Map

Severity of Impact							
	Significant	5	8=	4+		1=	
	High	4	9= 10-	6= 7-		2-	
	Medium	3	12= 13=	5+		3=	
	Low	2		11=			
	Insignificant	1					
Risk Map as of 03/22/2010 10:22 PM Company			1	2	3	4	5
			Remote	Low	Medium	High	Almost Certain
			Likehood of Occurance				

Color

Tolerance

🟩 Acceptable

🟨 Need Improveme

🟥 Unacceptab

Trend

-	+	=

Put Risks in Context

MetricStream

Summary and Call to Action

Summary - Call To Action

- A New Set of Risks
  - Understand Evolving Threat Landscape and Attack Profiles
- Defense Strategies
  - WEF Cyber Maturity and Framework
  - #1 Know the Impact
  - #2 Build Security In
  - #3 Continually Assess Risk
  - #4 Monitor and Analyze
  - #5 Plan Defensive Moves
  - #6 Leverage Advanced Analytics
  - #7 Share Information
  - #8 Collaborate in Groups
- Evolve to Cyber Risk Intelligence
  - Build a Cyber Intelligent Platform
  - Leverage Big Data
  - Aggregate Across the Extended Enterprise
  - Put Risks in Context
- Join the GCSC!
  - http://gcsc.georgetown.edu
  - http://s2erc.georgetown.edu/projects/cyberISE/

MetricStream Corporate Overview

Vision

Integrated Governance, Risk & Compliance (GRC) for
Risk-Driven Intelligence and **Better Business Performance**

Solutions

- Risk Management
- Corporate & Regulatory Compliance
- Policy & Procedure Management
- Internal Audit Management
- Case and Incident Management
- IT GRC
- Supplier & Vendor Governance
- Quality Management
- Environmental Health & Safety
- Business Continuity Management

Partners

Cognizant

CISCO

TATA CONSULTANCY SERVICES

pwc

IT UCF

Deloitte.

The Institute of Internal Auditors

Differentiators

- Technology - Enterprise GRC Platform – 9 Patents
- Breadth of Solutions – Single Vendor for all GRC needs
- Cross-industry Best Practices and Domain Knowledge
- ComplianceOnline.com – Largest Compliance Portal on the Web

Recognition

Gartner Leader in Gartner GRC Magic Quadrant: 2008 to present

FORRESTER Leader in Forrester GRC Wave

Q&A

Prof. Eric Burger MBA, PhD

Director, Georgetown Center for Secure Communications

Email - eburger@cs.georgetown.edu

Yo Delmar MBA, CMC, CISM, CGEIT

VP of GRC Solutions

MetricStream

Email - ydelmar@metricstream.com

Please submit your questions to the host by typing into the chat box on the lower right-hand portion of your screen.

Thank you for participating!

A copy of this presentation will be made available to all participants in next 48 working hours.
Please visit www.metricstream.com for more details on upcoming webinars.

MetricStream

Thank You

Contact Us:

Website: www.metricstream.com | **Email:** info@metricstream.com

Phone: USA +1-650-620-2955 | UAE +971-5072-17139 | UK +44-203-318-8554

Join us on RACE Group

Follow us on Twitter

Like us on Facebook

MetricStream