ODVA
2012
Industry Conference
and 15th Annual Meeting

CYBERSECURITY AND THE INDUSTRIAL ENTERPRISE

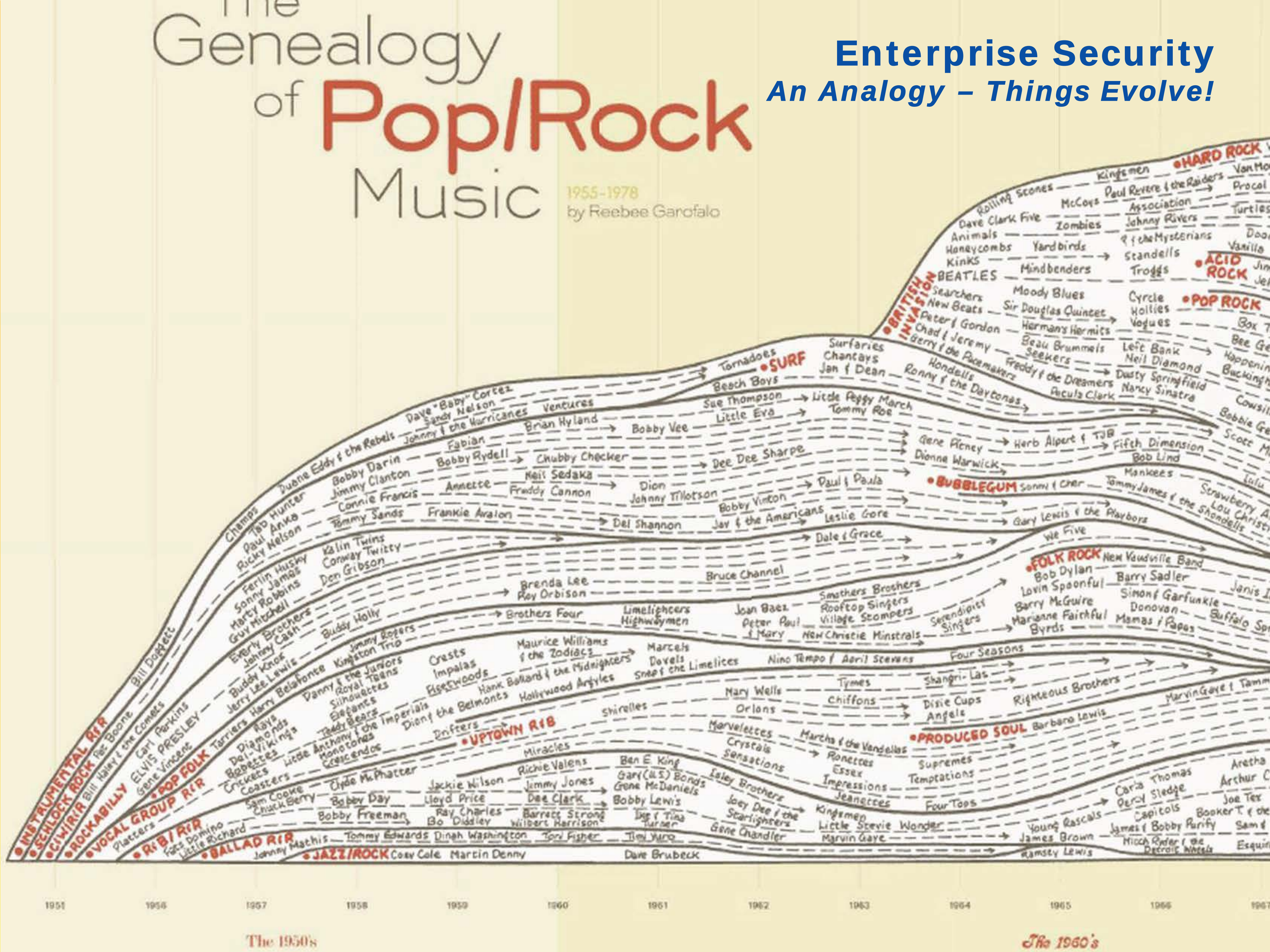
”LEVERAGING LESSONS LEARNED”

Derek E. Brink, BS, MBA, CISSP
Vice President and Research Fellow, IT Security and IT GRC
Aberdeen Group, a Harte-Hanks Company
Derek.Brink@aberdeen.com

General Session and 15th Annual Meeting of Members

Enterprise Security

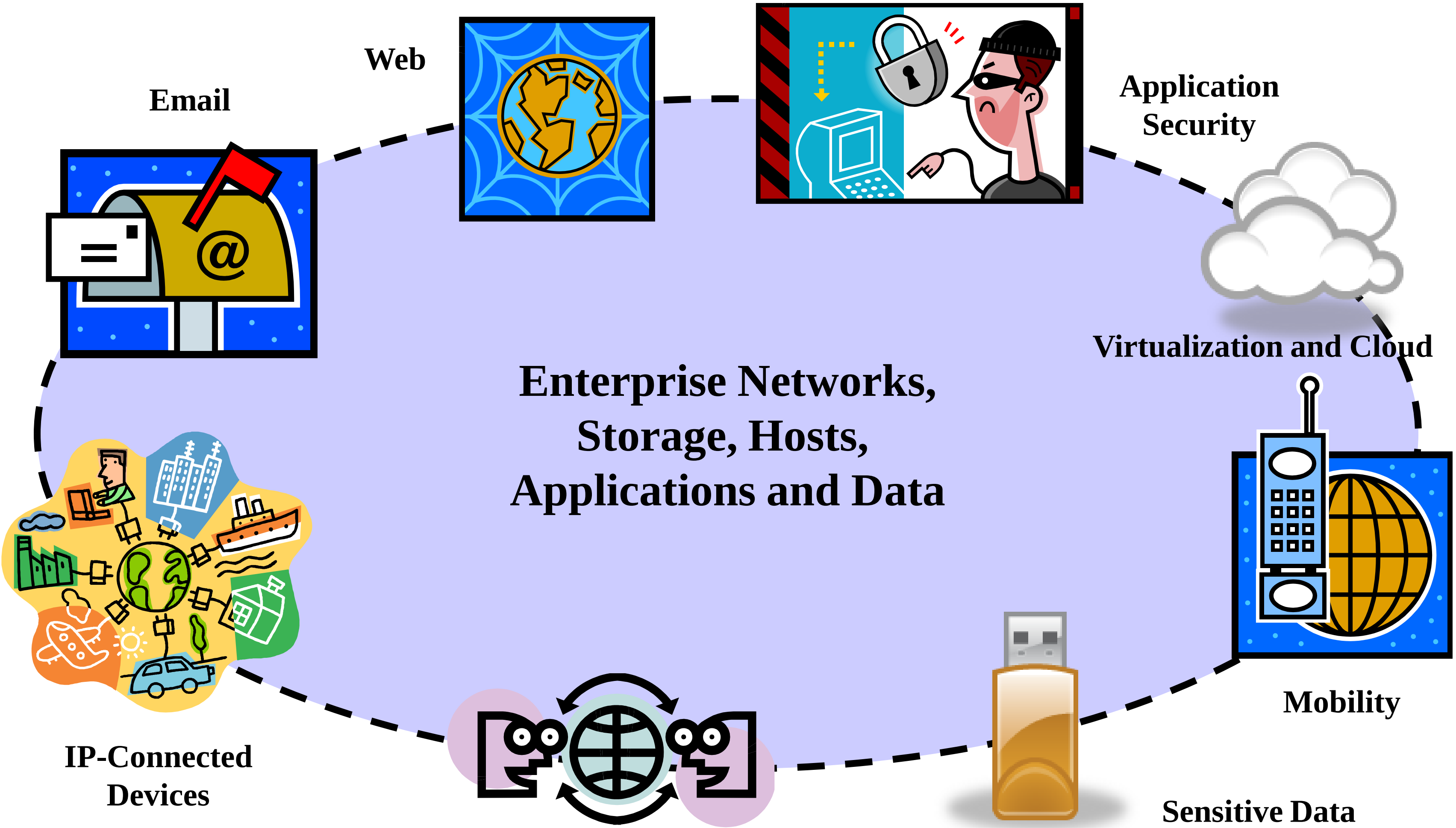
An Analogy – Things Evolve!



Business Context

Network Security: Enterprises Without Borders

- Traditional boundaries between the enterprise IT infrastructure and public IT infrastructure have become so porous that many embrace principle that there is no longer an enterprise border or perimeter at all.



Email

Web

Application Security

Virtualization and Cloud

Enterprise Networks, Storage, Hosts, Applications and Data

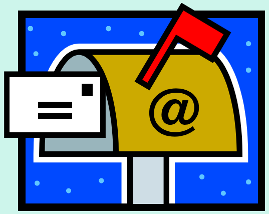
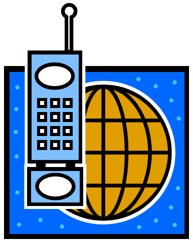
Mobility

IP-Connected Devices

Encapsulated / Tunneled Protocols

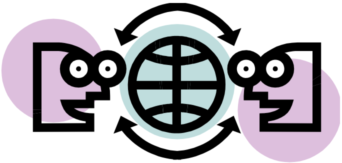
Sensitive Data

Erosion of the Traditional Network Perimeter (1)

	**Email** is a ready-made conveyance for pushing *malware*, *phishing* attacks and *blended threats* (i.e., seemingly innocuous email containing dangerous executables or web links) directly to end-users.
	Web access likewise sullies end-users with web-borne *malware*; *blended threats*, *drive-by downloads*, and *social engineering* exploits involving web URLs; and privacy and security risks from social networking sites and other real-time Web applications.
	Web-based **applications** have exploded in popularity, but have also spawned new waves of security vulnerabilities that target the ubiquitous Port 80.
	**Mobility** and wireless has become the “new normal”. On the one hand, mobility and anytime, anywhere network access enables end-user convenience, flexibility and productivity. On the other, it represents a set of under-recognized security risks to the organization’s IT infrastructure and critical data.

Erosion of the Traditional Network Perimeter (2)

Sensitive data supports the organization's unquenchable appetite for *productivity* and *collaboration*, but must simultaneously be protected and managed according to the relentless requirements for risk, audit and compliance.



IT solutions routinely permeate the network boundary by **encapsulating** security protocols within Web protocols, enabling transactions that **tunnel** through traditional perimeters or bypass them altogether – these are the “doggy doors” of the enterprise network. Widely deployed examples include secure file transfer solutions, which support protocols such as FTP, SFTP (FTP over SSH), FTPS (FTP over SSL or TLS), and HTTPS (HTTP over SSL or TLS).

New classes of **IP-enabled devices** – ranging from video surveillance cameras, to unified communications devices, to network printers, to industry-specific devices (e.g., in manufacturing, healthcare, transportation, retail) – are also proliferating across the enterprise network. The resulting jumble of computing platforms, network connectivity, applications and data comes with associated challenges in terms of visibility, control, risk and total cost.

Business Context

IT computing infrastructure has become considerably more complex in just the past couple of years

- **“Networks”** refers not only to electronic interconnections and protocols between systems – but also to social connections and collaboration between people, both within and across organizational boundaries

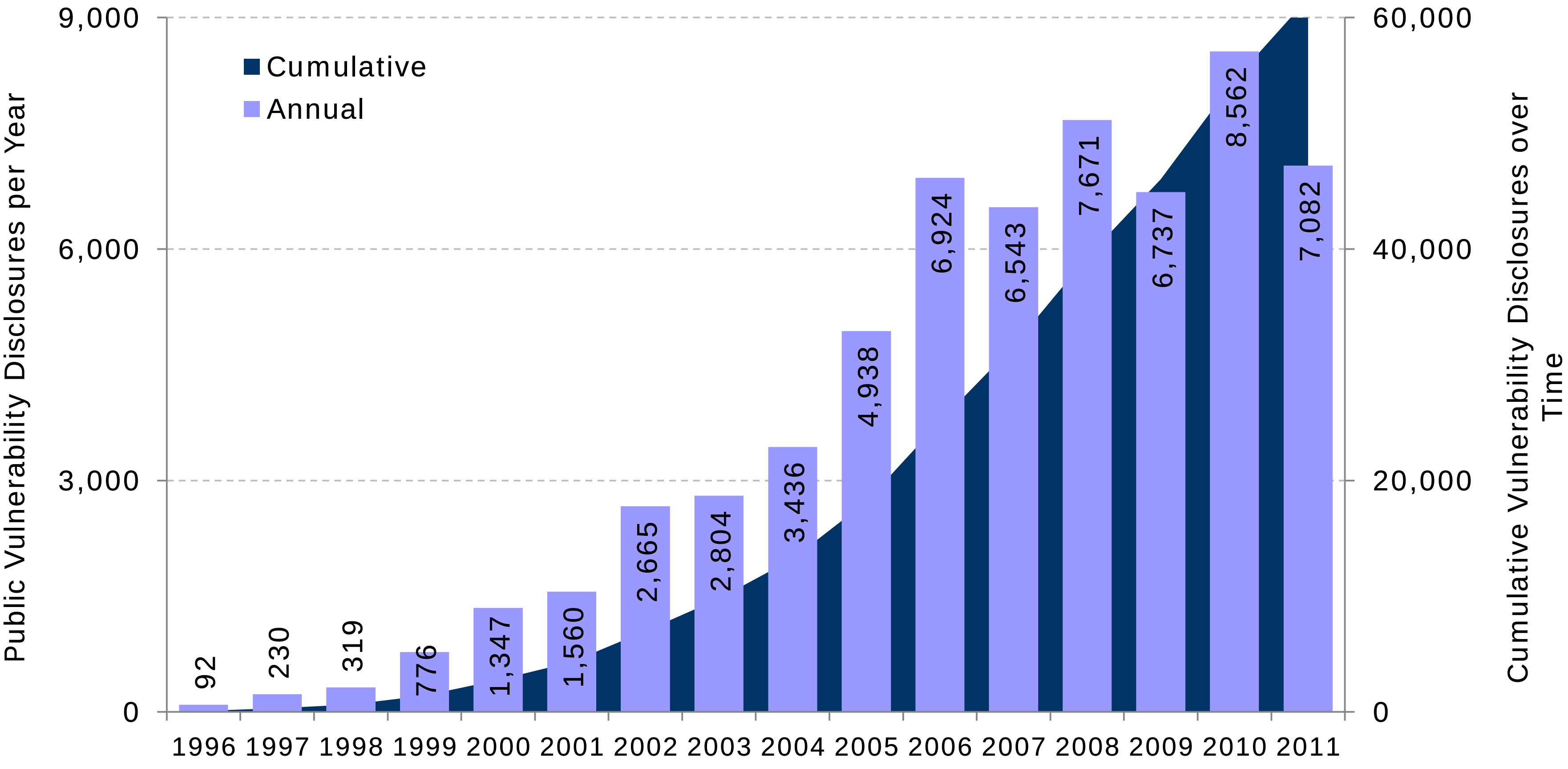
- **“Endpoints”** refers not only to traditional enterprise-provisioned devices – but also to highly mobile devices that are increasingly owned and managed directly by end-users – and increasingly to a host of other IP-enabled devices

- **“Back-end”** refers not only to the hosts, storage and applications within the enterprise datacenter – but also to virtualized resources in the datacenter or in the cloud

Business Context: Public Vulnerability Disclosures

2011 down from 2010; cumulative vulnerabilities tops 60,000

- Vendor patches available on the same day for 58% of vulnerabilities in 2011
- 38% of vulnerabilities are still unpatched – an improvement from 44% or higher over the last 5 years

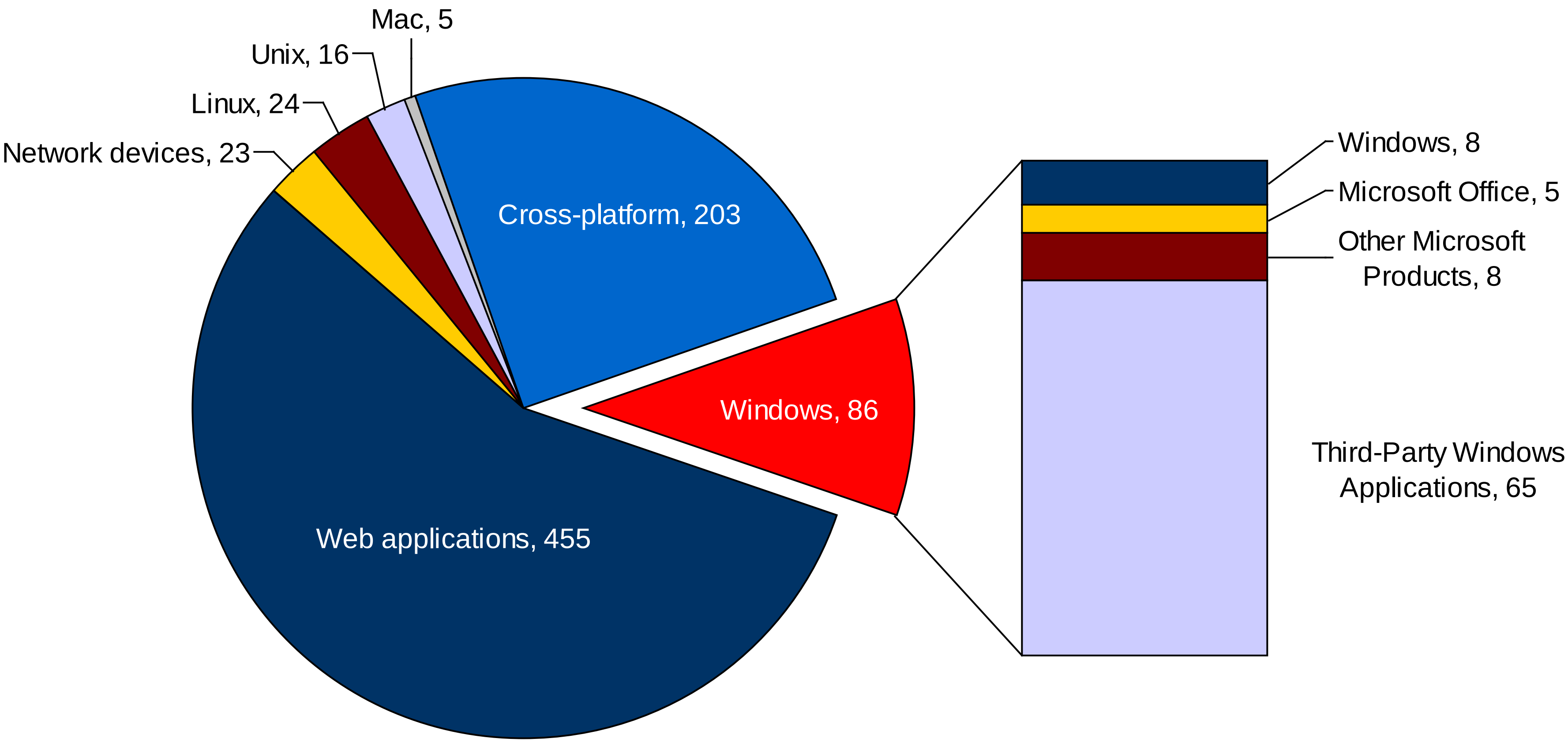


Source: IBM X-Force, March 2012

New Updates and Vulnerabilities Identified

in one typical 8-week period: >800

- There were 3-times more vulnerabilities in third-party Windows apps than in Windows, Microsoft Office and other Microsoft products combined – underscoring the importance of a comprehensive approach to VM
- SQL injections, cross-site scripting represented >60% of web application vuln, in spite of the OWASP Top 10



Source: Qualys, in partnership with SANS

New Updates and Vulnerabilities Identified
8 weeks in May-June 2010

Business Context

Changing circumstances call for a different approach

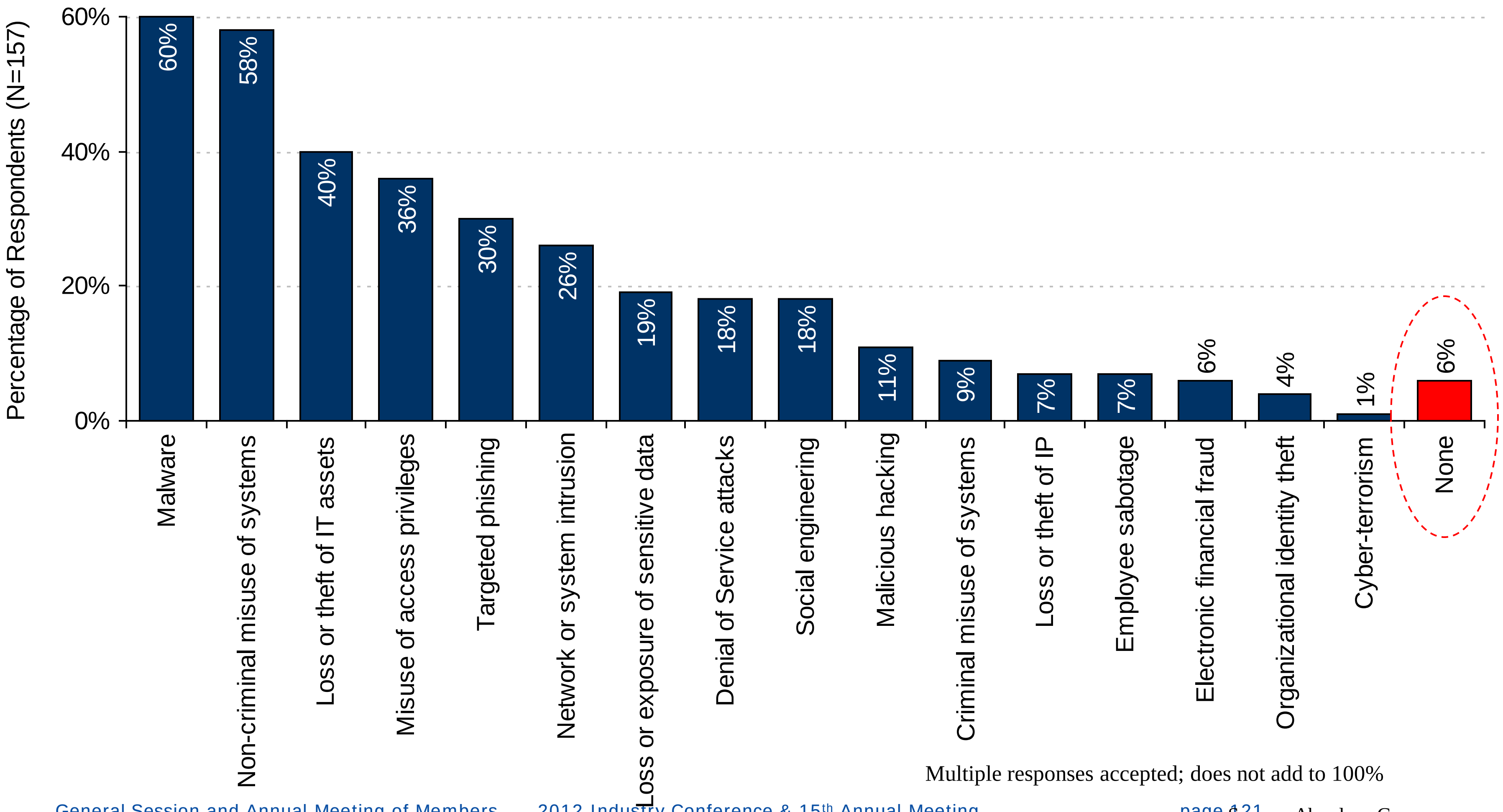
- One growing problem is that the traditional, *signature-based* approach to protecting against the vulnerabilities shown in the previous slides is under significant stress

- Most new malware represents slight variations of previously identified malware, a malevolent engineering process which is repeated continuously by attackers

- The traditional approach of determining what is “good” by detecting and subtracting what is known to be “bad” is not being discarded, but increasingly it must be augmented by complementary security technologies and a *defense-in-depth* approach

IT Security-related Incidents Experienced (last 12 months)

- 94% of all respondents experienced at least one IT Security-related incident in the past 12 months
- Average number of IT Security-related incidents experienced by participants in this study: 10.7

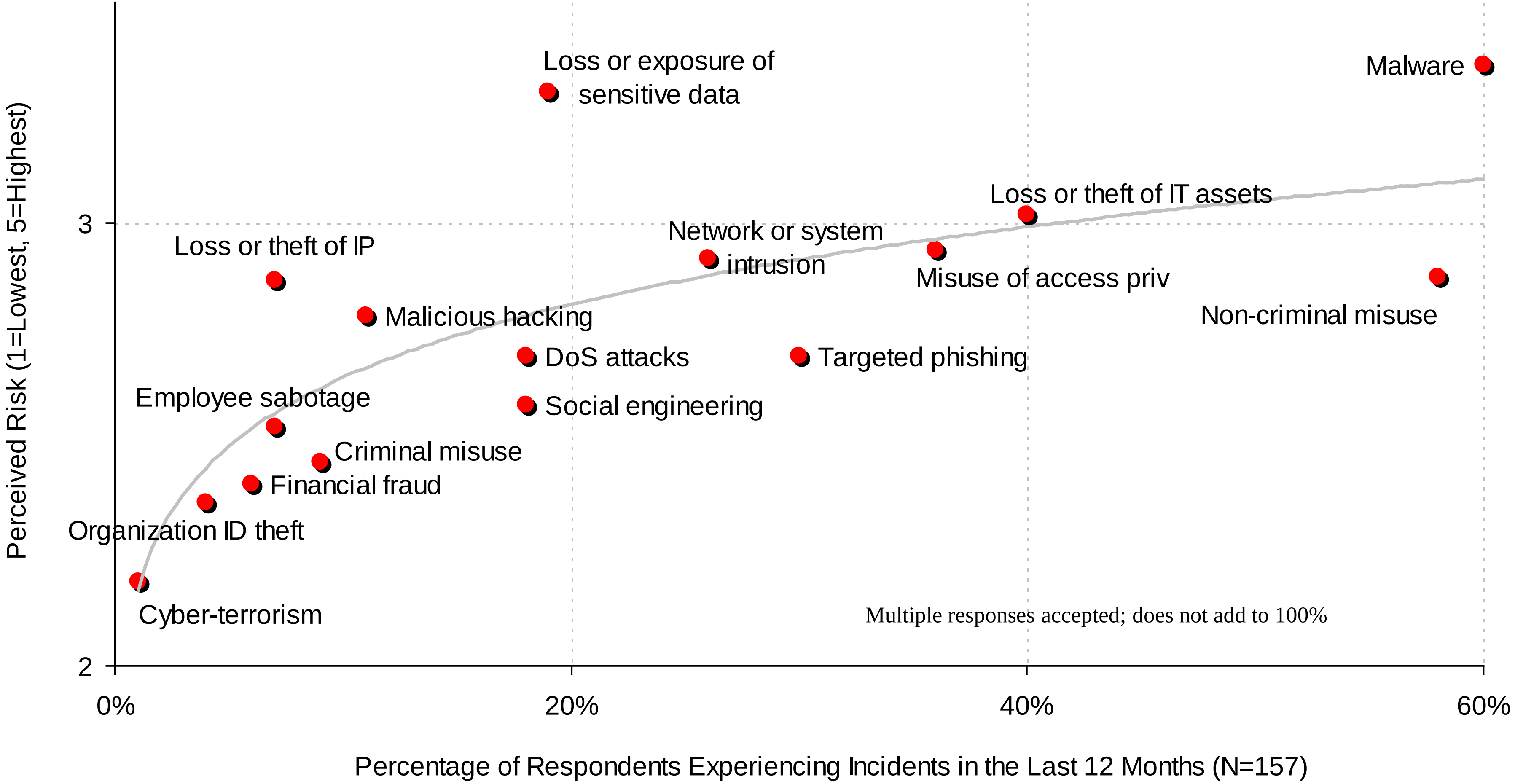


Multiple responses accepted; does not add to 100%

Source: Aberdeen Group

IT Security-related Incidents Experienced vs. Perceived Risk

- *Perception* of risk is moderately correlated with number of actual incidents; generally low (<3 on 1-5 scale)
- Highest perceived risks: **malware**, **loss or exposure of sensitive data**, **loss or theft of IT assets or IP, network or system intrusion, malicious hacking, misuse of access privileges**

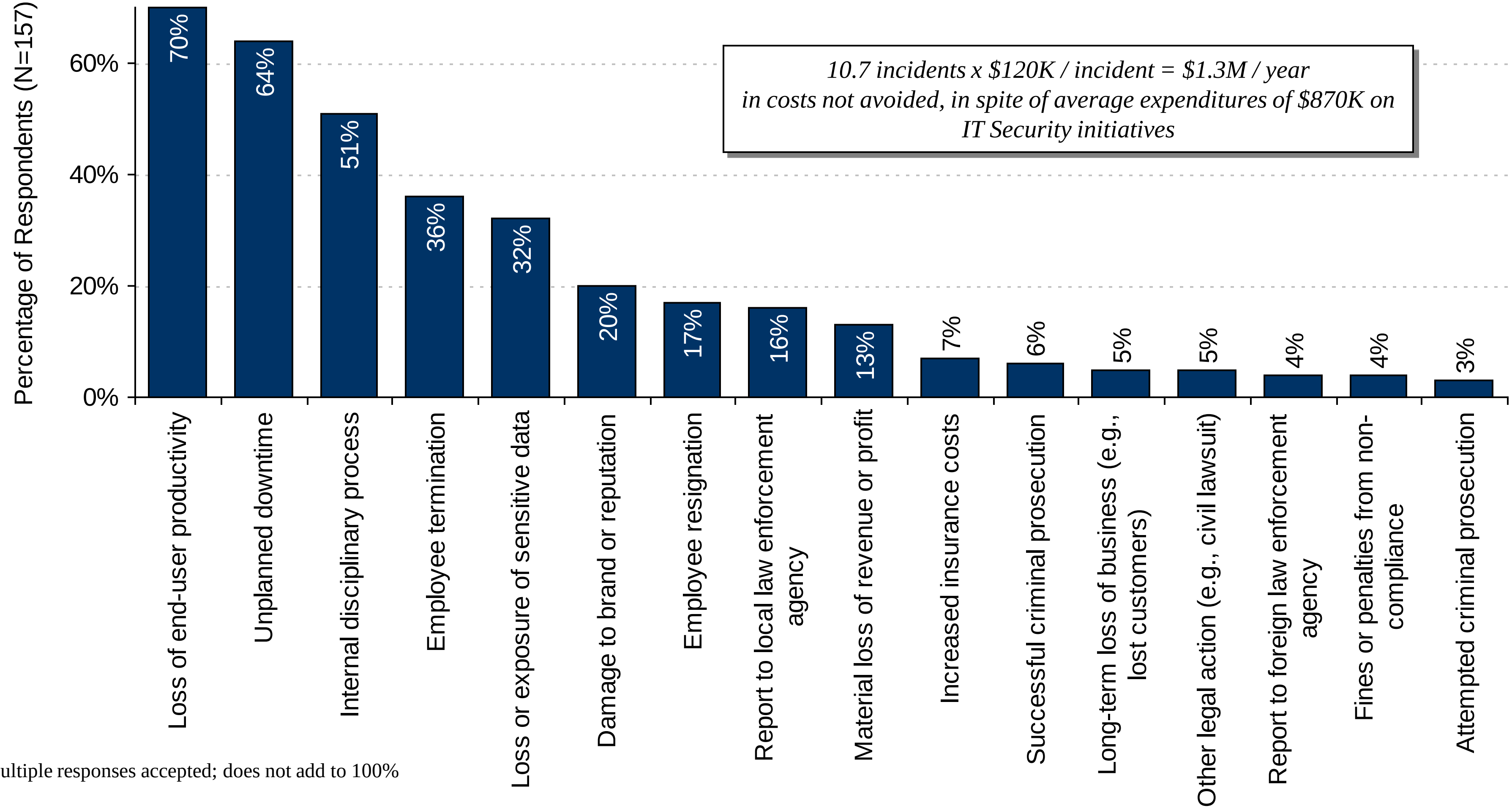


Multiple responses accepted; does not add to 100%

Source: Aberdeen Group

Consequences of IT Security-related Incidents Experienced

- Average financial impact per IT Security-related incident experienced by participants in this study: $120K
- Of financial losses in the last 12 months, average percentage attributed to IT Security incidents: 4.6%

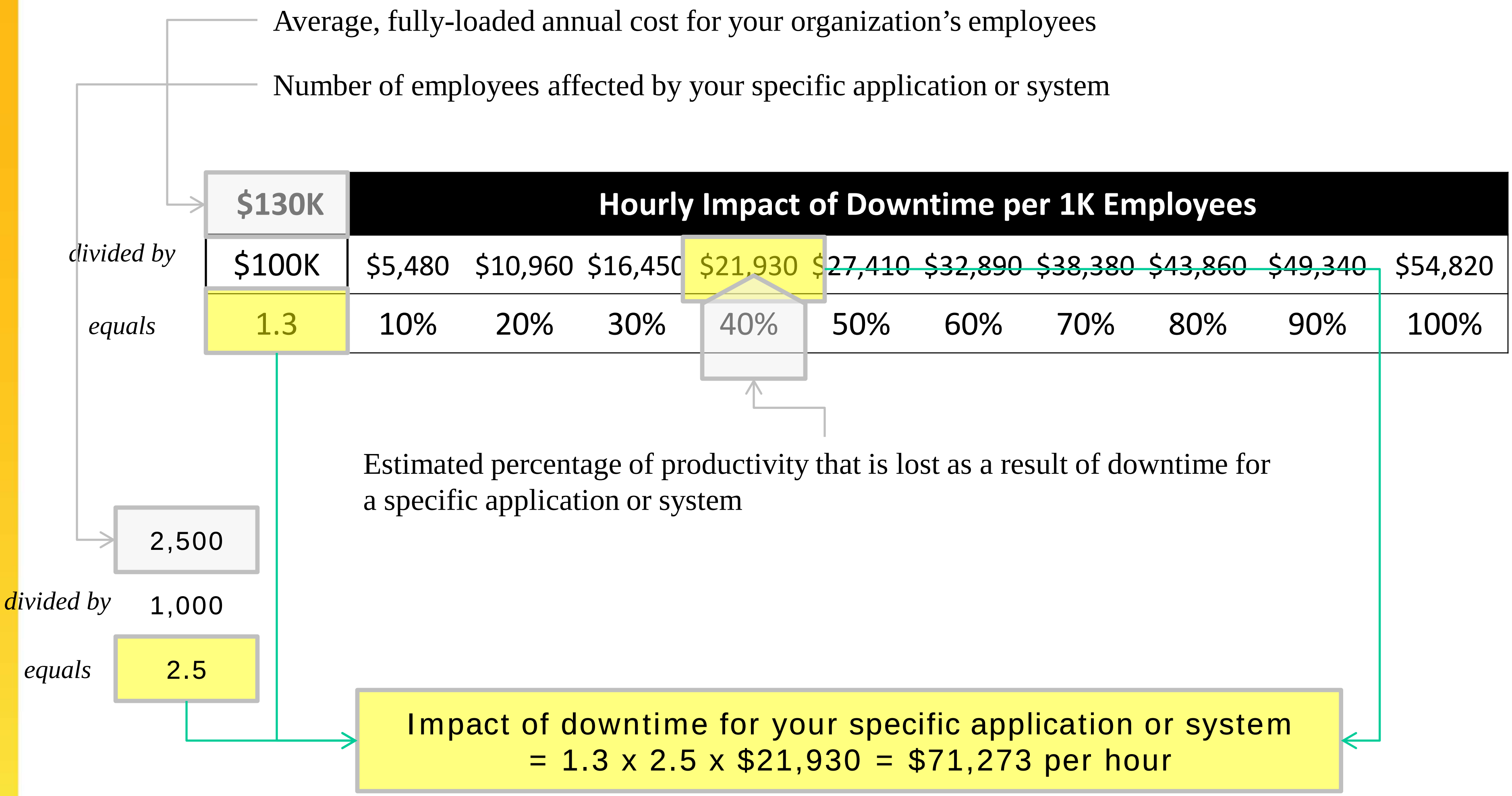


10.7 incidents x $120K / incident = $1.3M / year in costs not avoided, in spite of average expenditures of $870K on IT Security initiatives

Multiple responses accepted; does not add to 100%

Source: Aberdeen Group

Unplanned Downtime = Lost Productivity



Average, fully-loaded annual cost for your organization’s employees

Number of employees affected by your specific application or system

	$130K	Hourly Impact of Downtime per 1K Employees									
divided by	$100K	$5,480	$10,960	$16,450	$21,930	$27,410	$32,890	$38,380	$43,860	$49,340	$54,820
equals	1.3	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

Estimated percentage of productivity that is lost as a result of downtime for a specific application or system

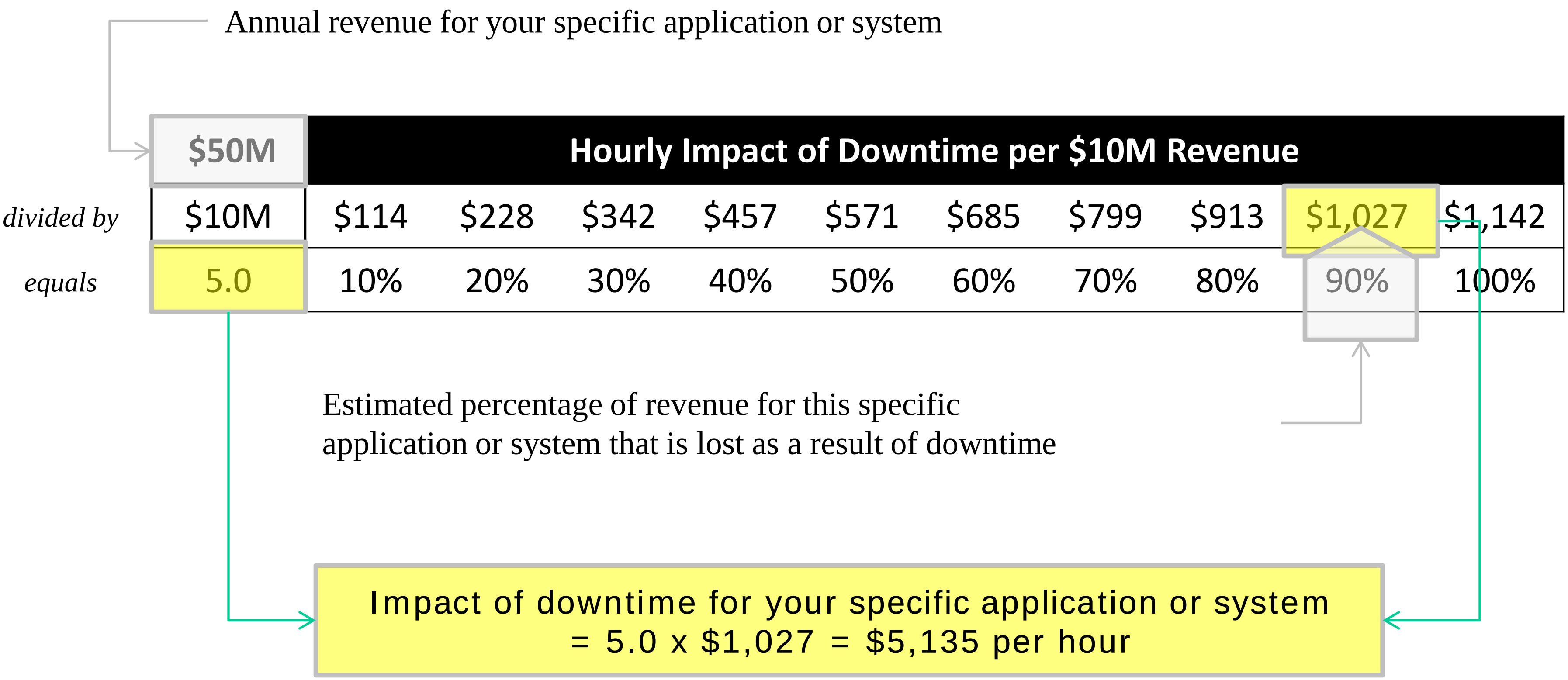
2,500

divided by 1,000

equals 2.5

Impact of downtime for your specific application or system
= 1.3 x 2.5 x $21,930 = $71,273 per hour

Unplanned Downtime = Lost Revenue



Annual revenue for your specific application or system

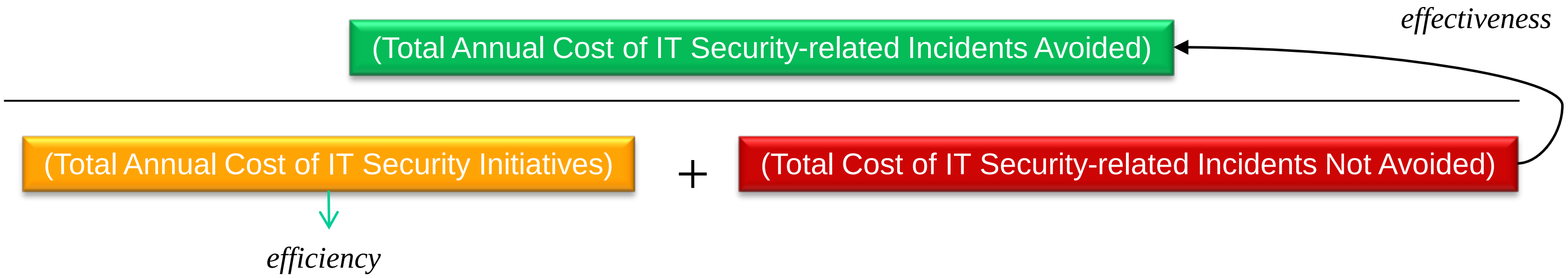
	$50M	Hourly Impact of Downtime per $10M Revenue									
divided by	$10M	$114	$228	$342	$457	$571	$685	$799	$913	$1,027	$1,142
equals	5.0	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

Estimated percentage of revenue for this specific application or system that is lost as a result of downtime

Impact of downtime for your specific application or system
= 5.0 x $1,027 = $5,135 per hour

Simple Framework for Evaluating Business Value

- IT Security return on annual investment:

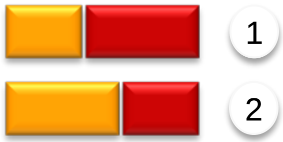


(Total Annual Cost of IT Security-related Incidents Avoided)

(Total Annual Cost of IT Security Initiatives) + (Total Cost of IT Security-related Incidents Not Avoided)

- Any investments in technologies and services that lower the total cost of the initiative (*efficiency*) and / or cause a greater shift from the denominator to the numerator in terms of security- and compliance-related incidents avoided (*effectiveness*) will have a positive impact on the return on investment

- The ratio of total costs invested to total costs not avoided is also a rough measure of the risk that is effectively accepted
  - E.g., which of the firms at right effectively accepted more risk?



LinkedIn, eHarmony (June 2012) >6 Million Passwords Compromised

- Perhaps the most disturbing aspect of these breaches is that neither LinkedIn nor eHarmony were using *salting* and *hashing* techniques – which have to be considered basic knowledge and best practice – prior to these incidents:
  - **LinkedIn:** "Affected members who update their passwords and members whose passwords have not been compromised benefit from the enhanced security we just recently put in place, which includes hashing and salting of our current password databases."
  - **eHarmony:** "Please be assured that eHarmony uses robust security measures, including password hashing and data encryption, to protect our members' personal information." [salting?]

Clearly, We as End-Users Must Take Responsibility for Continuing to Be So Stupid in Our Choice of Passwords

Within two days of the first public disclosure, some 165 thousand out of 6.46 million passwords (2.6%) from LinkedIn were already “cracked”:

1. link
2. 1234
3. work
4. god
5. job
6. 12345
7. angel
8. the
9. ilove
10. sex
11. jesus
12. connect
13. f*ck
14. monkey
15. 123456
16. master
17. b*tch
18. d*ck
19. michael
20. jordan
21. dragon
22. soccer
23. killer
24. 654321
25. pepper
26. devil
27. princess
28. 1234567
29. iloveyou
30. career

Yahoo! (June 2012)

- 453,492 passwords compromised

- The official statement said only that “the compromised information [usernames and passwords] was provided by writers who had joined Associated Content [now the Yahoo! Contributor Network] prior to May 2010, when it was acquired by Yahoo!”, and that “the compromised file … was not used to grant access to Yahoo! systems and services.”

- Note how carefully both parts of this statement are crafted to help us mentally minimize Yahoo’s responsibility for what happened
  - Why, these passwords were established before Yahoo acquired the company!
  - Why, the file wasn’t being used to grant access (which of course doesn’t mean that the usernames and passwords weren’t still valid)!
  - Why, this sounds like the Grinch explaining his actions to Cindy Lou Who, who was no more than two!

Yahoo! (continued)

- Evidently, the authentication information was stored *unencrypted* –

- In addition, it appears that the information was accessed by exploiting a SQL injection – which is perennially on the OWASP Top 10

- Why, one would think they would have known better!

Clearly, We as End-Users Must Take Responsibility for Continuing to Be So Stupid in Our Choice of Passwords

Swedish researcher Anders Nilsson posted his analysis of the Yahoo! passwords in his *Säkerhetsbloggen*:

Top 10 Passwords

- 123456
- password
- welcome
- ninja
- abc123
- 123456789
- 12345678
- sunshine
- princess
- qwerty

Top 10 Base Words

- password
- welcome
- qwerty
- monkey
- jesus
- love
- money
- freedom
- ninja
- writer

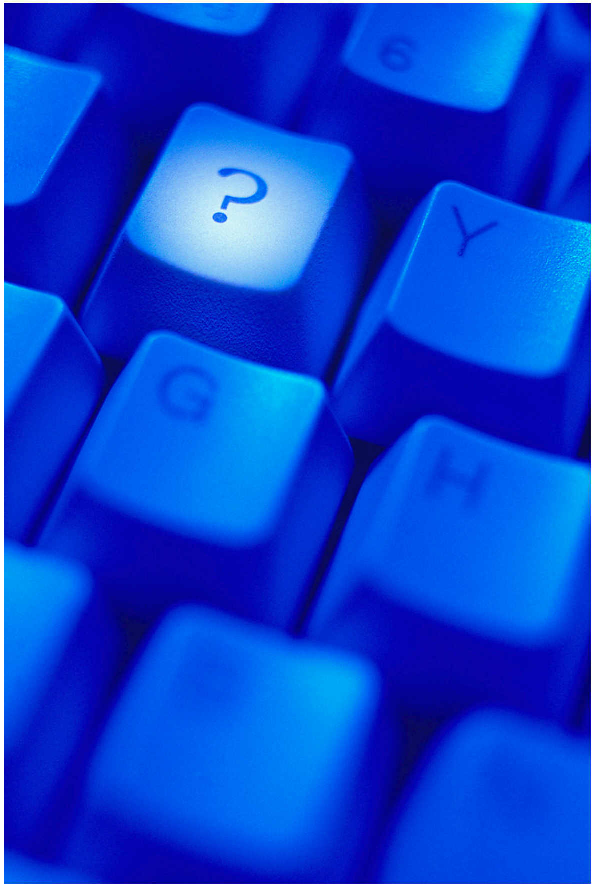
In the words of New York Yankee catcher Yogi Berra, “it’s another case of *déjà vu* all over again.”

Where is the Invisible Hand of the Market, or at least the Visible Hand of Management?

- At the same time, we really should expect world-class brands – such as Yahoo!, LinkedIn and eHarmony – to implement the most basic best practices and protections for our data, including salting and hashing for our passwords, and scanning and testing to find and fix the most common and well-known application vulnerabilities.
- And yet the natural forces between buyers and sellers did not cause this to be – until after a breach.

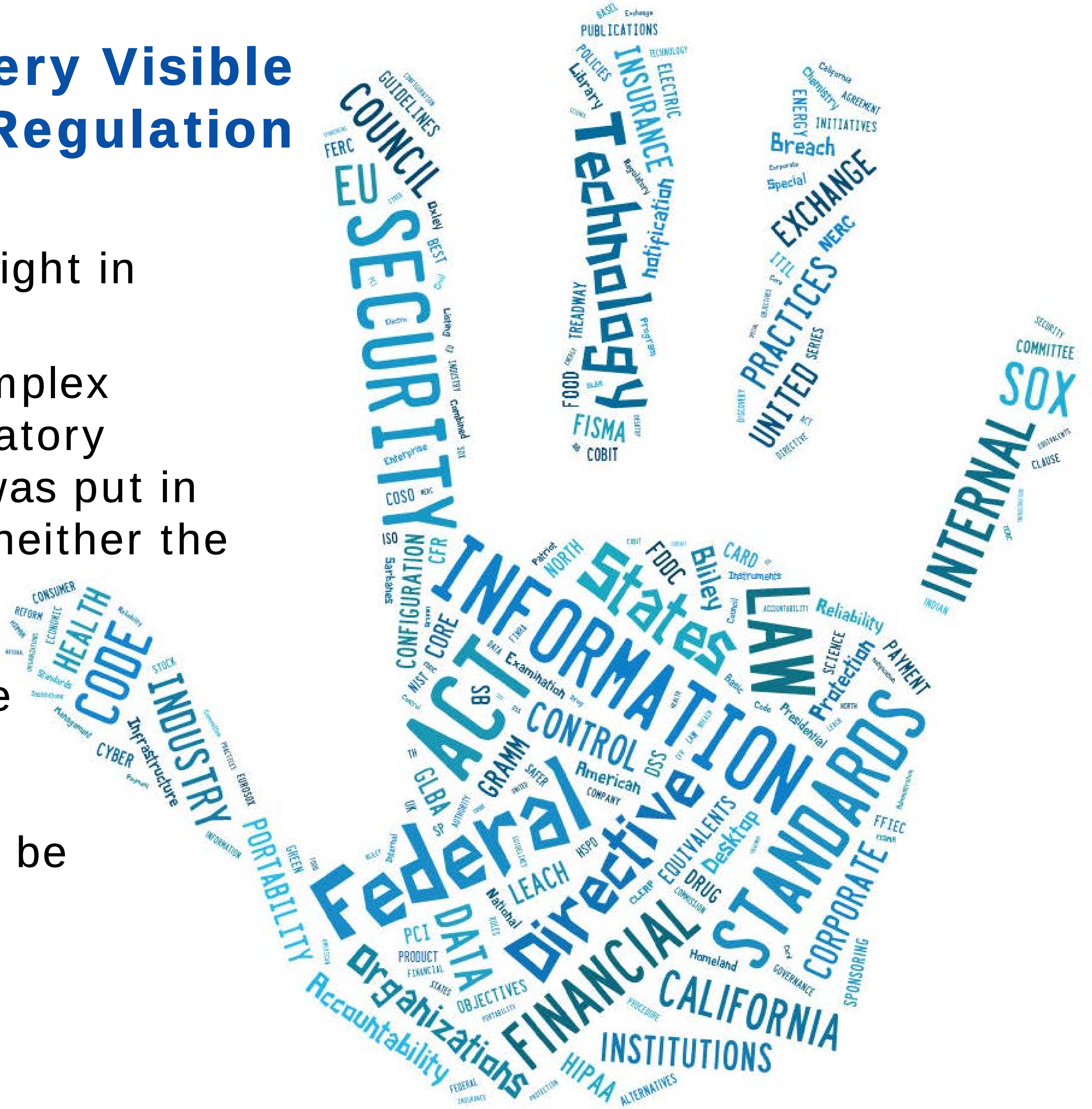
The Larger Question

- Is industry *capable* of self-regulation on IT Security matters?
- Or will corporate profit motives / indifference / incompetence continue to invite stronger *regulatory* mandates?



The Very Visible Hand of Regulation

- Is the answer right in front of us?
- Each of the complex matrix of regulatory requirements was put in place because neither the invisible hand of the market, nor the visible hand of management, was deemed to be adequate …



The Larger Larger Question

- **The question is magnified when it gets applied to critical infrastructure – i.e.,**
  - Power plants
  - Utilities
  - Pipelines
  - Transportation networks
  - Telecommunications networks
  - Hospitals
  - Financial systems
  - Other systems that people and businesses rely on for the essentials of daily life

A Current Example from the US.
This is a very, very visible hand indeed.

- On September 19, 2012, Senator John D. Rockefeller IV – frustrated at being unable to advance the revised Cybersecurity Act of 2012 through the Congress – wrote a letter to the Chief Information Officers of 500 leading companies, asking them to "help me understand your company's views on cybersecurity" by responding to eight questions within 30 days.

- This came just over a month after he urged President Barack Obama to institute the essential features of the act by Executive Order, bypassing the need for legislation.

- The likely alternative – as the Senator's letter to the CIOs makes clear – is "reactive and overly prescriptive legislation following a cyber disaster."

CIOs Who Received Sen. Rockefeller’s Letter

Exxon Mobil
ConocoPhillips
Berkshire Hathaway
Hewlett-Packard
Bank of America Corp.
Apple
Citigroup
Kroger
Wells Fargo
AmerisourceBergen
Walgreen
Home Depot
Target
PepsiCo
Dell
Dow Chemical
Kraft Foods
Best Buy
Amazon.com
Coca-Cola
Enterprise Products Partners
Sears Holdings
Sysco
DuPont
Supervalu
CHS
Ingram Micro
Liberty Mutual Insurance Group
Plains All American Pipeline
Sprint Nextel
Allstate
Tyson Foods
Phillip Morris International
3M
DirecTV
Avnet
International Paper
Staples
Raytheon
Emerson Electric
AMR
Goodyear Tire & Rubber
Manpower
U.S. Bancorp
Freeport-McMoRan Copper & Gold
Nucor
Baker Hughes
United States Automobile Association
Whirlpool
Cummins
J.C. Penney
Altria Group
Paccar
Computer Sciences
PNC Financial Services Group
Amgen
CenturyLink
L-3 Communications
Viacom
PPG Industries
Dollar General
Duke Energy
Lear
Anadarko Petroleum
Baxter International
Community Health Systems
Chubb
Kellogg
Consolidated Edison
PPL
ConAgra Foods
Smithfield Foods
Health Net
Monsanto
Starbucks
Liberty Interactive
Office Depot
Textron
Entergy
Nordstrom
Dick's Sporting Goods
United Stationers

SAIC
Ameriprise Financial
Applied Materials
Jacobs Engineering Group
Newmont Mining
Unum Group
EOG Resources
Sempra Energy
Automatic Data Processing
Tenet Healthcare
URS
Las Vegas Sands
Visa
NRG Energy
Caesars Entertainment
Micron Technology
Bed Bath & Beyond
Ball
Discover Financial Services
Henry Schein
Gilead Sciences
Hertz Global Holdings
Energy Transfer Equity
Reliance Steel & Aluminum
W.W. Grainger
AECOM Technology
Williams
Corning
MGM Resorts International
Campbell Soup
Oshkosh
Ameren
Regions Financial
Eastman Chemical
Dole Food
Spectrum Group International
BorgWarner
Interpublic Group
Targa Resources
Ecolab
Celanese
Jarden
Weyerhaeuser
NuStar Energy
CMS Energy
Dillard's
Anixter International
Omnicare
Advance Auto Parts
Expeditors International of Washington
Cognizant Technology Solutions
WellCare Health Plans
Hershey
Ryder System
Rockwell Automation
Harris
CBRE Group
PVH
Exelis
Fidelity National Information Services
Emcor Group
Ralph Lauren
Starwood Hotels & Resorts
St. Jude Medical
CH2M Hill
Laboratory Corp. of America
SPX
Rock-Tenn
Momentive Specialty Chemicals
Catalyst Health Solutions
Harley-Davidson
Pitney Bowes
Frontier Communications
Big Lots
Timken
Casey's General Stores
Biogen Idec
Host Hotels & Resorts
Western & Southern Financial Group
Charles Schwab
Insight Enterprises
BrightPoint

El Paso
Alliant Techsystems
Aleris
Erie Insurance Group
Molina Healthcare
Wal-Mart Stores
General Motors
Fannie Mae
AT&T
Verizon Communications
CVS Caremark
Cardinal Health
Costco Wholesale
Procter & Gamble
INTL FCStone
American International Group
Medco Health Solutions
Boeing
Johnson & Johnson
WellPoint
United Technologies
Intel
Lowe's
Merck
Express Scripts Holding
Safeway
Walt Disney
FedEx
Google
United Continental Holdings
Humana
Oracle
World Fuel Services
TIAA-CREF
News Corp.
HCA Holdings
Deere
Nationwide
Time Warner
Publix Super Markets
Tech Data
Travelers Cos.
Alcoa
Halliburton
Massachussetts Mutual Life Insurance
Fluor
Xerox
Cigna
Arrow Electronics
Nike
EMC
Time Warner Cable
Exelon
Capital One Financial
AES
Apache
Jabil Circuit
FirstEnergy
Eaton
Bank of New York Mellon
Progressive
NextEra Energy
Oneok
Qualcomm
General Mills
National Oilwell Varco
Dominion Resources
Loews
Navistar International
Omnicom Group
Texas Instruments
Waste Management
Dean Foods
Land O' Lakes
Yum Brands
Parker Hannifin
Coventry Health Care
Penske Automotive Group
Thermo Fisher Scientific
eBay
Fidelity National Financial
FMC Technologies

Marsh & McLennan
Avon Products
Huntsman
Public Service Enterprise Group
First Data
Xcel Energy
R.R. Donnelley & Sons
Stanley Black & Decker
Peter Kiewit Sons'
Genworth Financial
Liberty Global
Whole Foods Market
BB&T Corp.
CDW
GameStop
Western Digital
CarMax
Enbridge Energy Partners
Western Refining
Reinsurance Group of America
AGCO
Principal Financial
Owens & Minor
Family Dollar Stores
Dover
Ashland
Assurant
Autoliv
Peabody Energy
AutoZone
Steel Dynamics
Commercial Metals
TravelCenters of America
Thrivent Financial for Lutherans
Boston Scientific
Masco
Quest Diagnostics
Broadcom
Pantry
Tenneco
Franklin Resources
Alpha Natural Resources
DaVita
Cameron International
Cliffs Natural Resources
NII Holdings
Fifth Third Bancorp
Agilent Technologies
Advanced Micro Devices
AK Steel Holding
McGraw-Hill
Precision Castparts
Corn Products International
Core-Mark Holding
Mylan
Consol Energy
CF Industries Holdings
Group 1 Automotive
Eastman Kodak
Mutual of Omaha Insurance
Newell Rubbermaid
Dr Pepper Snapple Group
Pacific Life
Health Management Associates
SLM
Auto-Owners Insurance
Mohawk Industries
Foot Locker
Spectra Energy
Kelly Services
Kindred Healthcare
NCR
Live Nation Entertainment
Centene
Clorox
Con-Way
Wynn Resorts
Gannett
Allegheny Technologies
W.R. Berkley
Vanguard Health Systems
YRC Worldwide

NetApp
CVR Energy
SunGuard Data Systems
Yahoo
Susser Holdings
CIT Group
Celgene
J.M. Smucker
Nash-Finch
McKesson
Chevron
General Electric
Ford Motor
Valero Energy
J.P. Morgan Chase & Co.
International Business Machines
UnitedHealth Group
Freddie Mac
Archer Daniels Midland
Marathon Petroleum
MetLife
Microsoft
Pfizer
State Farm Insurance Cos.
Caterpillar
Comcast
United Parcel Service
Prudential Financial
Lockheed Martin
Sunoco
Cisco Systems
Morgan Stanley
Abbot Laboratories
Hess
Honewell International
Goldman Sachs Group
Delta Air Lines
New York Life Insurance
Aetna
General Dynamics
American Express
Murphy Oil
Tesoro
Northrop Grumman
McDonald's
Macy's
Rite Aid
Northwestern Mutual
Eli Lilly
Occidental Petroleum
TJX
Aflac
Hartford Financial Services Group
Bristol-Myers Squibb
Kimberly-Clark
United States Steel
Union Pacific
Kohl's
Illinois Tool Works
Southern Company
Colgate-Palmolive
Danaher
TRW Automotive Holdings
Medtronic
Southwest Airlines
HollyFrontier
Marathon Oil
American Electric Power
PG&E Corp.
Global Partners
Gap
CBS
DISH Network
Toys "R" Us
AutoNation
Ally Financial
Aramark
US Airways Group
Edison International
Genuine Parts
Telephone & Data Systems
Meritor

Marriott International
Sara Lee
Icahn Enterprises
CSX
Chesapeake Energy
Devon Energy
Aon
Praxair
Norfolk Southern
H.J. Heinz
Lincoln National
Guardian Life Insurance Company of America
Synnex
Limited Brands
C.H. Robinson Worldwide
State Street Corp.
Air Products and Chemicals
Mosaic
SunTrust Banks
Motorola Solutions
VF
KBR
BlackRock
DTE Energy
Estée Lauder
Sherwin-Williams
Crown Holdings
Ross Stores
Reynolds American
CenterPoint Energy
Stryker
Kinder Morgan
Republic Services
Great Atlantic & Pacific Tea
Visteon
Coca-Cola Enterprises
Hormel Foods
Sonic Automotive
Becton Dickinson
Dana Holding
Universal Health Services
Darden Restaurants
Owens-Illinois
Cablevision Systems
Charter Communications
OfficeMax
Energy Future Holdings
Barnes & Noble
Calpine
Avery Dennison
MasterCard
Dollar Tree
Sanmina-SCI
Terex
American Family Insurance Group
Amerigroup
Mattel
Symantec
CC Media Holdings
Wesco International
PetSmart
UGI
MeadWestvaco
NiSource
Shaw Group
Pepco Holdings
Avis Budget Group
General Cable
O'Reilly Automotive
Seaboard
SanDisk
Sealed Air
Domtar
Booz Allen Hamilton Holding
Avaya
Western Union
Allergan
Graybar Electric
Owens Corning
Bemis
Rockwell Collins
KeyCorp

Similar Activity in the EU

- **IMPROVING NETWORK AND INFORMATION SECURITY (NIS) IN THE EU**
  - ▶ Network and information systems have become essential for economies and societies
  - ▶ Incidents are on the rise and have serious consequences
  - ▶ Critical sectors include finance, health, energy and transport
  - ▶ Public consultation open from 23 July 2012 to 15 October 2012

Enabling Technologies Commonly Used in Network Security (illustrative)

Threat detection and protection

- Firewall
- Intrusion detection / prevention
- Network vulnerability scanning

Content protection

- Email monitoring / filtering
- Web monitoring / filtering
- Content monitoring / filtering (DLP)
- Virtual private network

Beyond Traditional Firewalls

Illustrative Solutions Landscape / Definitions

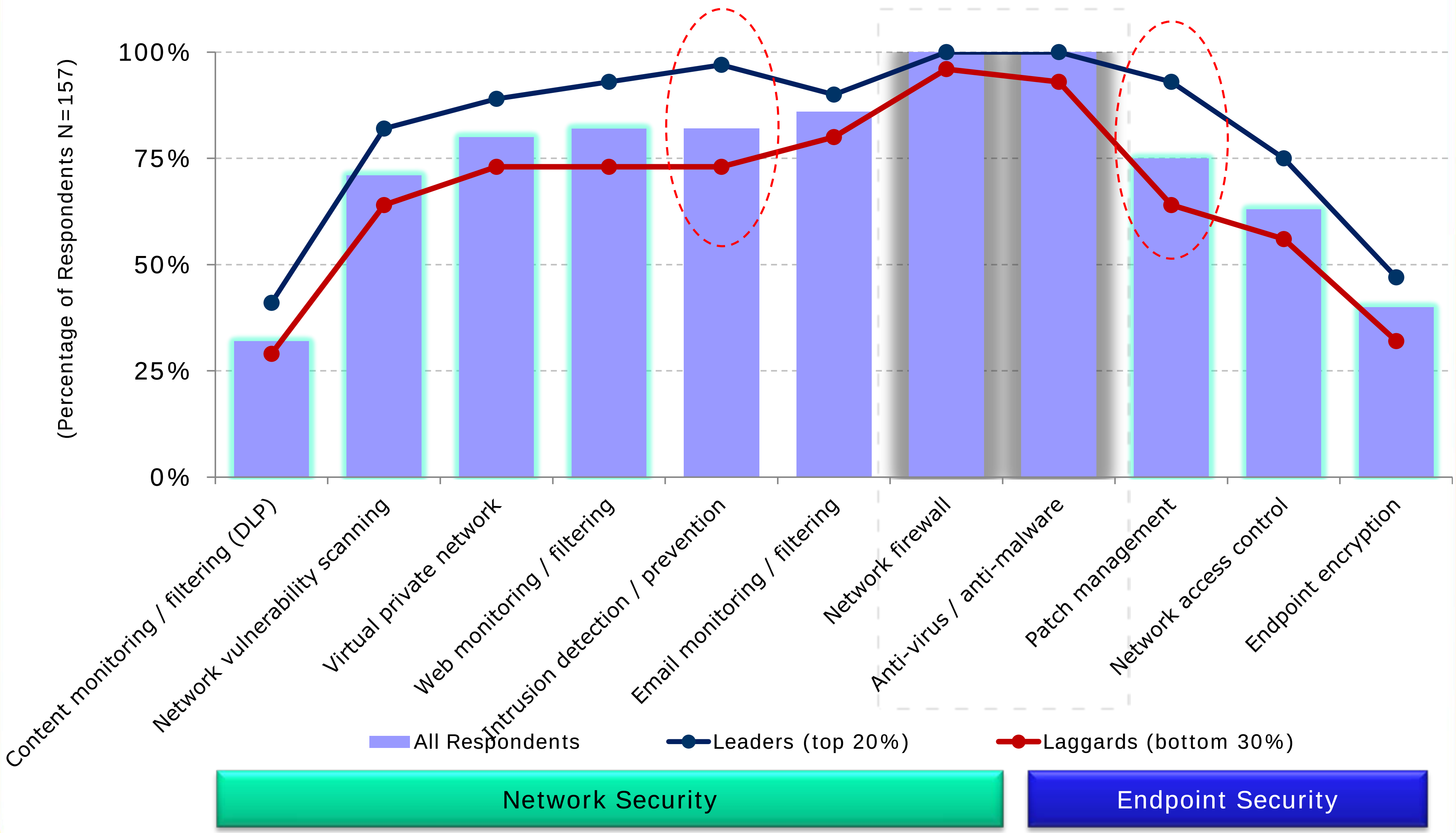
Firewalls plus advanced Intrusion Prevention Systems	Because there are so many open paths through traditional network firewalls, most companies have augmented them with complementary technologies (e.g., *intrusion detection / prevention*). A growing problem is that the traditional (i.e., *signature-based*) approach for these complementary technologies is under significant stress in its own right, which is why advanced capabilities such as *behavioral analysis* and *deep packet inspection* will become increasingly important.
Unified Threat Management (UTM)	The term *unified threat management* was coined to describe a single network appliance that combines multiple network security technologies – typically *firewall*, *intrusion detection / prevention*, *virtual private network*, *monitoring and filtering* (email, web, content), and *anti-virus* – with a common, unified management interface.
Next-Generation Firewalls	Next-generation firewalls typically integrate *firewall* and *intrusion detection / prevention* capabilities; they are distinguished by leveraging **stateless** protocols to increase **application-specific** visibility and to enable application-specific and identity-specific policies and controls.

Enabling Technologies Commonly Used in Endpoint Security (illustrative)

	Protect	Manage
Data	□ File / folder encryption □ Full-disk encryption □ Self-encrypting drives □ Endpoint device / port controls □ Data loss prevention □ USB drive encryption □ Email encryption	□ Online backup/recovery (files) □ Online backup/recovery (image) □ Remote erasure / “wiping”
Applications	□ Email monitoring / filtering □ Web monitoring / filtering □ Application whitelisting □ Browser protection	□ Software distribution □ Software inventory / usage □ Application virtualization
Networks	□ Personal firewalls □ Intrusion detection / prevention (HIPS) □ Network access control	
Platforms	□ Anti-virus / anti-malware □ Patch management □ Configuration / change management □ Physical device security □ Anti-Theft technology □ Platform hardening	□ Remote disablement / “kill” □ Patch management □ Configuration / change mgmt □ Asset management □ Asset tracking and recovery

All Organizations Have Deployed Firewalls and Anti-Virus

Leaders (top 20%) have also deployed additional network security and endpoint security solutions to a higher degree than laggards (bottom 30%)



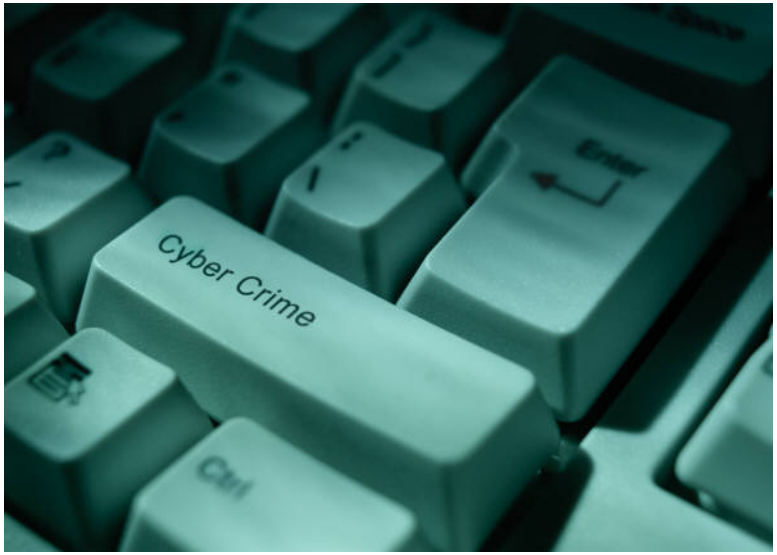
Source: Aberdeen Group

Final Thoughts

Both the infrastructure and the threat landscape have very recently become considerably more complex

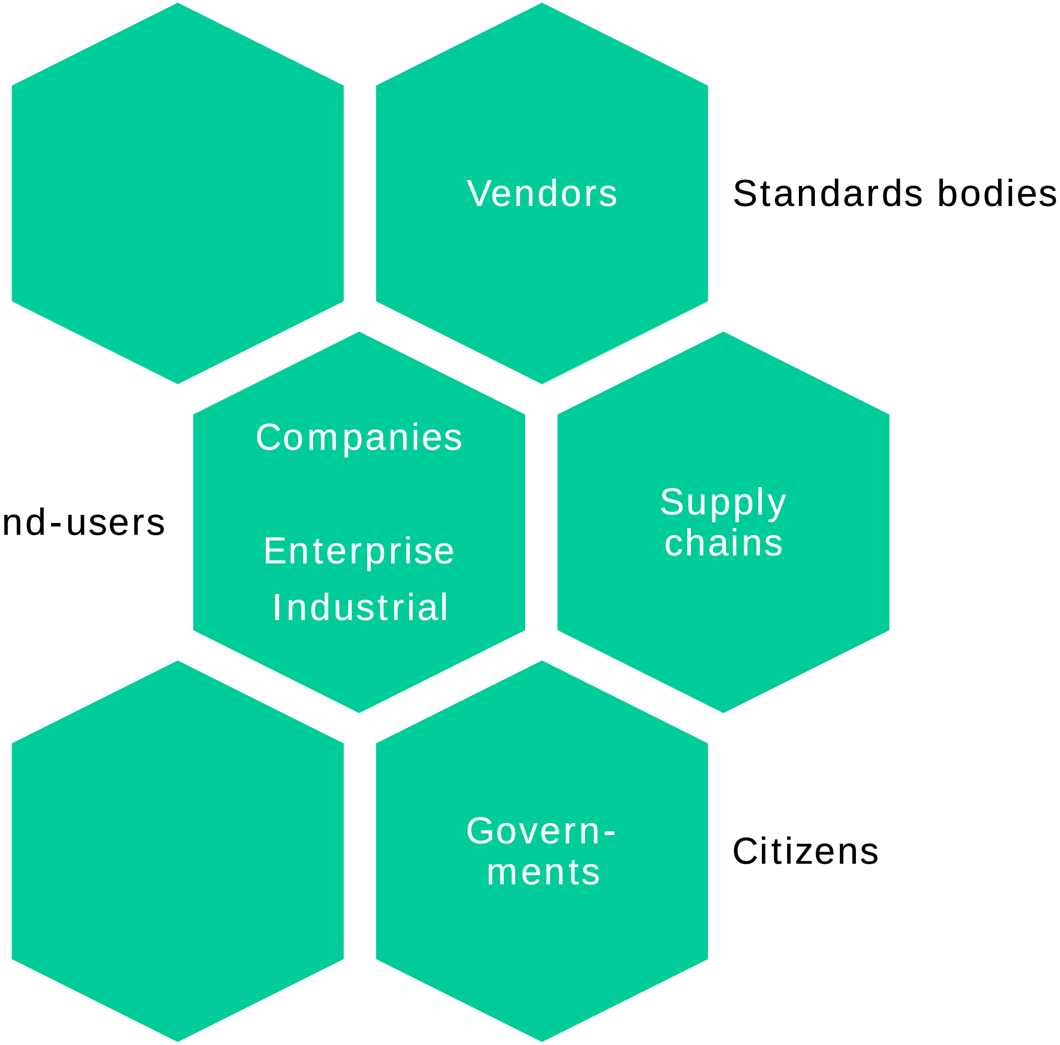
Who – or what – is the Enemy?

- Attackers – which range from insiders, to petty criminals, to organized crime; and from terrorists, to anti-establishment "hacktivists," to state-sponsored initiatives?
- Flawed technology?
- Poor implementation?
- Lack of education?
- End-users?
- Vendors?
- Supply chains?
- Regulators?
- Ourselves?
- All of the above?



Collaboration and Information-Sharing

"If you want to go fast, go alone. If you want to go far, go together."



ODVA
2012
Industry Conference
and 15th Annual Meeting

Questions / For More Information

Commercial / Marketing Services

Robert Ellington
Robert.Ellington@aberdeen.com
+1-617-854-5236

Research

Derek E. Brink, BS, MBA, CISSP
Vice President and Research Fellow,
IT Security and IT GRC
Derek.Brink@aberdeen.com

www.aberdeen.com

General Session and
15th Annual Meeting of Members