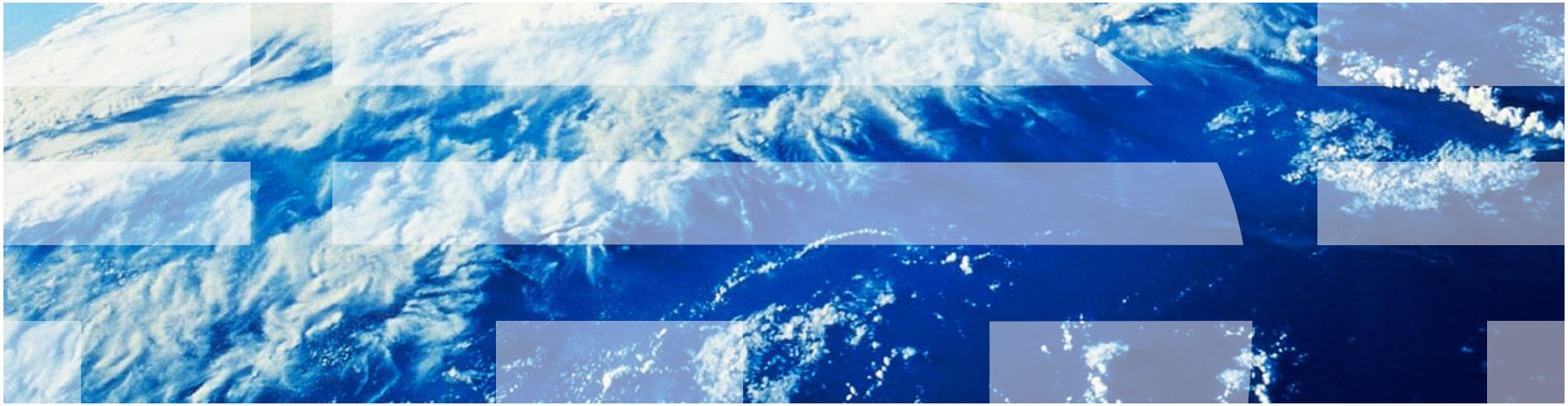
Paul R. Lazarr, CISSP, CISA, CIPP, CRISC
Managing Consultant, Cybersecurity & Privacy

June 19, 2012

The Continuity / Security Convergence

Presentation to ISSA-DC



Cyber Threat, Social Media and the Connected Society – Resiliency, Security & Speed Matter.

…globalization of society and business has increased our reliance on **uninterrupted intelligent interconnected** computing, communications and organizational models.

Today's agenda:

1. The resurgence of business continuity & resilience…continuity is cool again!
2. The importance of business continuity to security
3. Integration of security, business continuity, enterprise risk mgmt and privacy - why this makes sense
4. How BCP can make a good Security practitioner stronger.

Threat Scenario's …

…. Continuity & Security Practitioners face similar risks.

External Threat

▪ ***Power failures*** ▪ ***Data Breach (IP /PCI /PII)*** ▪ ***Natural disasters*** ▪ ***Economic upheaval*** ▪ ***System Failure*** ▪ ***Epi or Pandemic***	▪ Cyber Espionage / Crime ▪ Malware ▪ Denial of service (DOS) ▪ Sophisticated, organized attacks – APT ▪ *Civil Unrest/Boycotts*
▪ Vulnerable Systems, People or Processes ▪ Data leakage ▪ Human error or carelessness ▪ ***Data Breach (IP / PCI /PII)***	▪ Developer-created back door ▪ Information theft ▪ Insider fraud ▪ *Workplace violence*

Inadvertent ***Deliberate***

Insider Threat

Trends – *Breach Costs Continue to Grow*

Year	Avg Total Cost Per Breach	Avg Per Record
2008	$6,655,758	$202
2009	$6,751,451	$204
2010	**$7,241,899**	**$214**

- Regulatory Compliance Increasing Cost but changing focus from Mitigation to Prevention
- 88% of respondents in 2010 had at least 1 data breach. Of these:
  - 23% had one incident (decreased t pts from 2008)
  - 40% had 2-5 incidents (decreased 4 pts from 2008) - 4 incidents = $29 Million
  - **25% had more than 5 incidents (Doubled between 2008 and '09) - 6 incidents = $44 M**
- Top 2010 breach in study cost an organization **$35.3 million** up $4.8 Million (15% increase)
- Least costly breach was $780,000, up $30K (4% increase)

Source: Ponemon Inst. 2010 Annual Study: U.S. Cost of a Data Breach

2011 Example:

- *Sony expected breach response will cost $176 Million in 2011;* ***DIRECT COST (source: WSJ 7/28/11)***

Sony 2011 - The Perfect Storm; A Business Case for Resiliency

2011 a painful year for Sony – Natural Disasters, Economic and Business Threats, Criminal PII, PCI, IP Data Breaches PSN Outages…

- 2 Natural Disasters (Tsunami & Thailand floods)
- Business: Strong Yen, Weak TV Market; TV products not competitive
- Multiple Breaches (PCI & PII) impact several divisions
- Multiple Playstation Network Outage April 20 – early June
- Response missteps & lost opportunities
- Oct ’11 -more security trouble; 93k PSN accounts unauthorized access
- 1/23/12 – Downgraded by Moody’s to Baa1 from A3.
- Projected loss of $2.8B USD for fiscal year ending in March 31st

Resilience –

"… the national focus should be on resilience… Resilience – the capability to anticipate risk, limit impact and bounce back rapidly – is the ultimate objective of both economic security and corporate competitiveness. Causes count less than the agility and flexibility to mitigate risk and manage outcomes"

- Debra van Opstal, *The Resilient Economy* (Council on Competitiveness)

A Resilient organization can adapt to circumstance and work around disruptions to achieve its critical business objectives under all conditions.

"Hyper-Resilient" organizations don't just fully recover from a crisis, but use the crisis as a catalyst for positive transformation

- Clair and Dufffresne

"Because security systems fail so often, the ***nature of the failure is important***. Systems that fail badly are brittle, systems that fail well are resilient. A resilient system is dynamic; it might be designed to fail only partially; it might adjust to changing circumstances"

- Bruce Schneier, "Beyond Fear"

Attributes of Resilient Organizations

- Convergence of multiple disciplines (creating synergy)
  - Physical Security,
  - Information Security
  - Business Continuity (includes resiliency)
  - Crisis Management
  - Risk Management
  - Privacy
- *All Threats* approach to resiliency and continuity
- Emergence of Enterprise Security Risk Management (ESRM) – security managing non-security (business) risk; holistic approach
- Embrace failure; Learn from it; Use it to strengthen the business
- Pay attention to the “near misses”
- Resilient organizations approach to holistic risk management.
- Leadership, Culture, People, Systems & Settings (Gartner)
- Everyone is a risk manager; Security is everyone’s job

Security as a Value Add – Brand Protection

- Innovation => Intellectual Property (IP) => Products => Jobs
- IP accounts for 75% of value of the Fortune 500 (Source: WIPO)
- 66% of companies assets are not physical; e.g. virtual
- Advanced Persistent Threat (APT)
  - Logistics + Targeting + Persistence = APT
  - APT = Acquire IP or $$ for financial gain, industrial espionage and/or spying
  - 70-80% of APT victims are notified by external parties
  - You can't stop APT; you can make it hard to maneuver once inside (WINv7)
- Enterprise Security Risk Management (ESRM) role in brand protection through cross functional teams. (Source: Conference Board)
- 50% of Fortune 500 CISO have staff dedicated to ESRM – evaluating, prioritizing mitigating non-security risks (Source: Conference Board)

Security, Risk and Recovery – How did they fair?

- Sony PlayStation Network, Sony Online Entertainment Breaches
- Victims of LulzSec / Anonymous / WikiLeaks
- Nortel – State Sponsored Cyber Espionage
- TEPCO – Fukashima, Japan – risks known & unknown
- BP / TransOcean / Haliburtan (BP - $8B in claims paid, Reuters 2/23)
- Carnival Cruise Lines
  - Carnival expects FY ’12 - $144 impact to net income & $355M to profit, WSJ/CNN 1/31/12)
- SAIC – Unencrypted TriCare Backup Tape
  - Books FY ’12 - $10M loss provision (low end) (source: SAIC 10-K)
- Global Payments
  - Will release estimated financial impacts on 7/26 investor call

Did these organizations exhibit Agility, Flexibility, effective risk management, crisis response….

- 25% of organizations that experience a total IT outage go bankrupt immediately.
- 85% of organizations that lose their data center for more than 10-days are bankrupt within 1-year. (NARA study)

The greatest disruptions are those that have rarely or never occurred and thus could not be accurately anticipated

How BCP can make a good Security Practitioner Stronger

- Enterprise Perspective
  - Holistic View of enterprise, both systems and business processes
  - You can't recover it if you don't know how its put together
  - Bridge business and IT communities
  - Insight into core business and mission critical business outputs
  - Connecting the dots (business & data flows) inside and out
- Business Resumption, IT recovery, Crisis Management
- Integration and Synchronization – Conductors/directors view.
- Testing
- Risk Management (business, IT and industry)
- Risk Based Resource Prioritization

Personal tips & techniques:

- Know thy business!
  - What are your organizations core competencies & market space?
  - How is success measured by the business (corp/division score cards)?
  - Key competitors / market pressures
  - Your Organization/client in the news (google news feeds)
  - Identify Critical Data & Assets (PII, PCI, BSI, IP)
  - Understand critical supply chain; data flows, ingress egress points
- Integrate with Change Mgmt (IT & business)
- Problem Mgmt - Outage/Disruptions Post Mortums; wealth of knowledge
- Integrate with key corporate partners:
  - Legal
  - Privacy
  - Enterprise Risk Management (new: ESRM)
  - Database & Data Warehouse
  - Networking & Telecommunications
  - Corporate Communications
- Periodically Reassess Risks, Threats, Resiliency and Readiness

Sources:

1. 2010 Annual Study: U.S. Cost of a Data Breach
   (The Ponemon Institute & Symantec)
   www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

2. 2010 Data Breach Investigations Report
   (Verizon RISK Team & the USSS)
   www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

3. 2011 Data Breach Investigations Report
   (Verizon RISK Team, USSS, & DNHTCU
   www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

4. 2010 Data Breach Investigations Report
   (Verizon RISK Team & the USSS)
   www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Contact Information

Paul R. Lazarr, CISSP, CISA, CIPP, CRISC
Managing Consultant, Cybersecurity and Privacy
IBM Global Business Services - US Federal Team

Office: 202-649-2188
Mobile: 703-628-0024

prlazarr@us.ibm.com
lazerp13@gmail.com

BIO

Paul R. Lazarr, CISSP, CISA, CIPP, CRISC

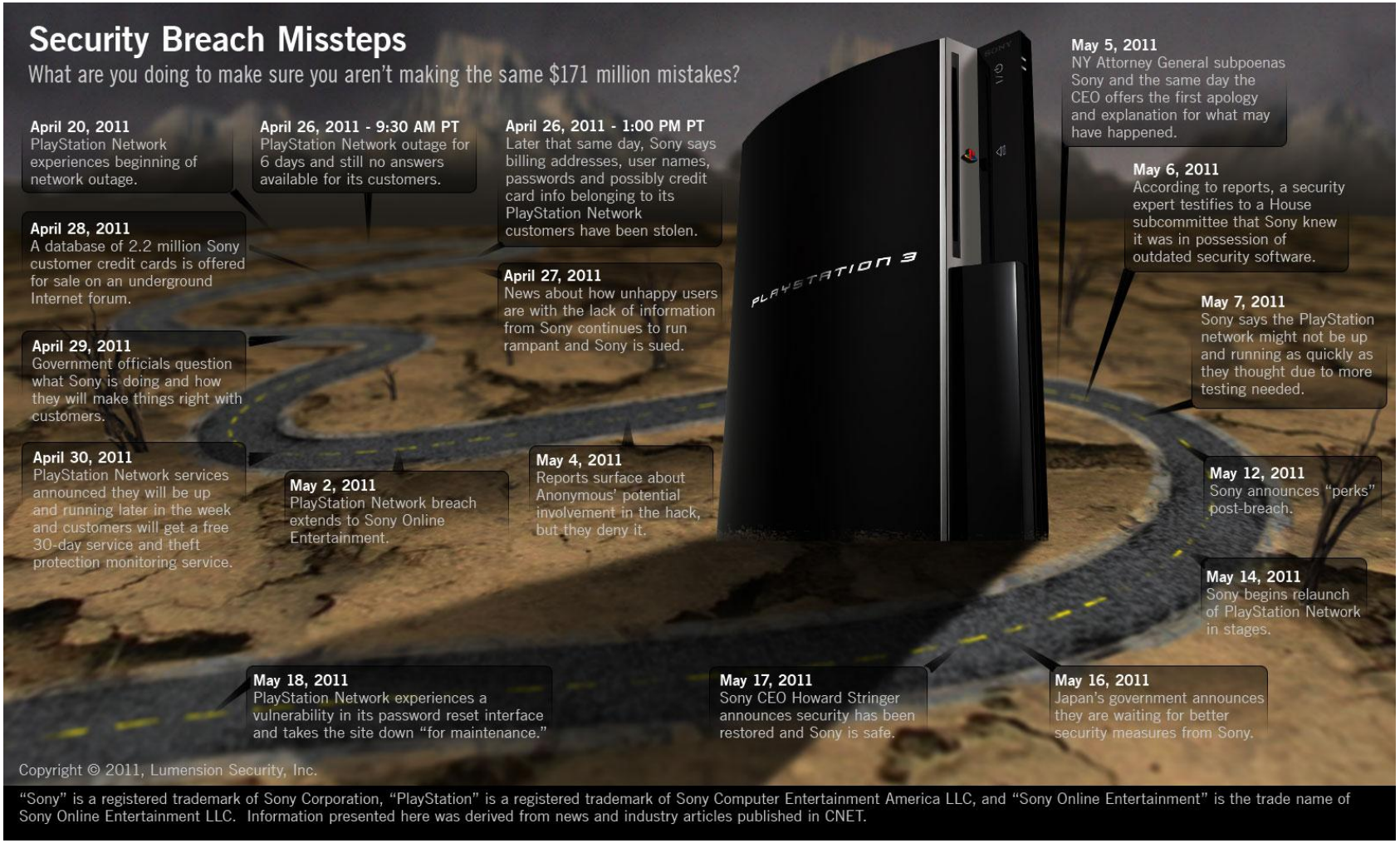
Professional Profile

Paul Lazarr has over 25 years of IT experience that includes: information security, privacy, business continuity, risk management and process re-engineering. Currently, Paul is a Managing Consultant in the U.S. Federal IBM Cybersecurity and Privacy Practice leading the DR & COOP supporting an large transformation project. Paul's 10+ years of BCP experience covers traditional IT Disaster Recovery, Crisis Management and Business Resumption for several fortune 25 companies. Previously, he led the compliance program within the College Board's Information Security Office. In this capacity, Mr. Lazarr oversaw Payment Card Industry – Data Security Standards (PCI-DSS) compliance awareness, reporting, assessment(s) and remediation activities. Additionally, he was responsible for the creation of a privacy awareness practice within the IT organization. Mr. Lazarr is and active member of ISACA National Capital Area Chapter, International Association of Privacy Professionals, USSS Electronic Crimes Task Force, Infragard, as well as an avid follower of numerous security, risk management, and privacy blogs.

Additional Content

Backup Material & Additional Content.

Sony – The most expensive breach in history?



Source: Lumension Security, Inc.

2012 Verizon Data Breach Investigations Report

Highlights (2011 data – Verizon, USSS, DNHTCU, AFP, IRISSCERT, PCeU)

Who was Responsible (Agents):

98%	External Agents	**(+6%)**
4%	Insiders	(-13%)
<1%	Business Partners	(<>)
58%	Activist Groups	

Commonalities among breach events

79%	Victims – targets of opportunity	(-4%)
96%	Not considered highly difficult	**(+4%)**
94%	Compromised servers	(**+18%**)
92%	Discovered by an external party	**(+6%)**
97%	Avoidable with simple controls	(**+1%**)
96%	[PCI loss victims] Not yet PCI compliant	(**+7%**)

How they did it (Agent Actions)

81%	Hacking	(**+31%**)
69%	Utilized Malware	(**+20%**)
10%	Physical Attacks	(-19%)
7%	Social Tactics	(-4%)
5%	Privileged Misuse	(-12%)

Mitigation Focus Areas:

- Eliminate unnecessary data; Keep track of sensitive data
- Ensure essential [key] controls are met
- Double check the above again
- Assess remote access services
- Test and review web applications
- Audit user accounts and monitor privileged activity
- Monitor [review] and mine event logs

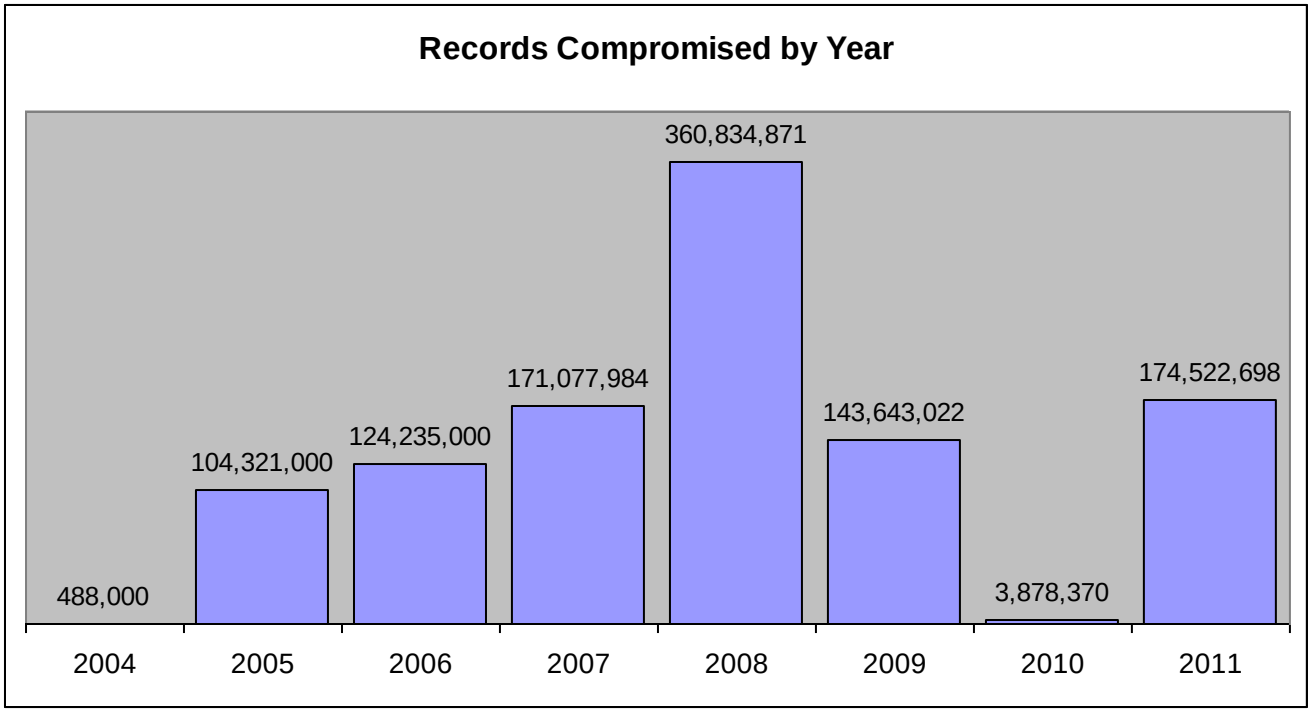
2012 - 855 incidents / 174 million records

Additional Contributors:

USSS *– United States Secret Service (2007-2011)*
DNHCTU *– Dutch National High Tech Crime Unit (2006-2011)*
AFP *- Australian Federal Police* ***(NEW 2012)***
IRISSCERT *– Irish Reporting & Information Security Service* ***(NEW 2012)***
PCeU *– Police Central e-Crime Unit, London Metropolitan Police* ***(NEW 2012)***

Records Compromised by Year

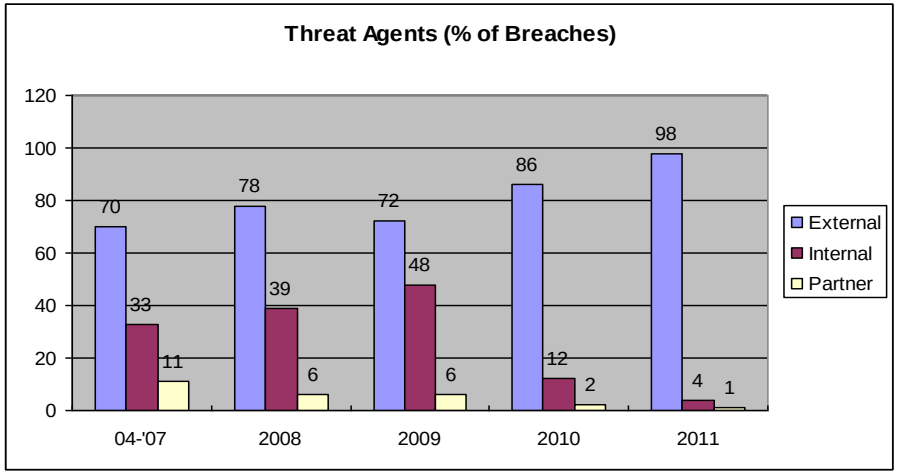
2012 Verizon Data Breach Investigation Report (DBIR)



Additional Contributors:

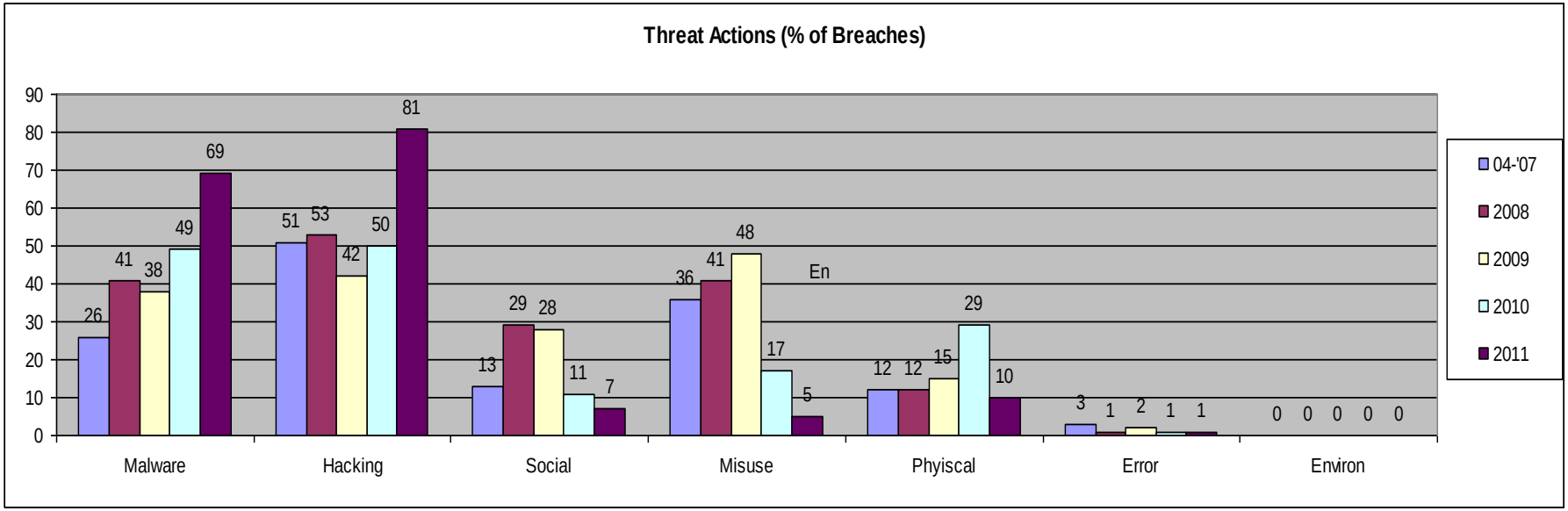
USSS *– United States Secret Service* ***(2007-2011)***
DNHCTU *– Dutch National High Tech Crime Unit* ***(2006-2011)***
AFP *- Australian Federal Police* ***(NEW 2012)***
IRISSCERT *– Irish Reporting & Information Security Service* ***(NEW 2012)***
PCeU *– Police Central e-Crime Unit, London Metropolitan Police* ***(NEW 2012)***

The Threat – Agents and Actions (2004 to Present)

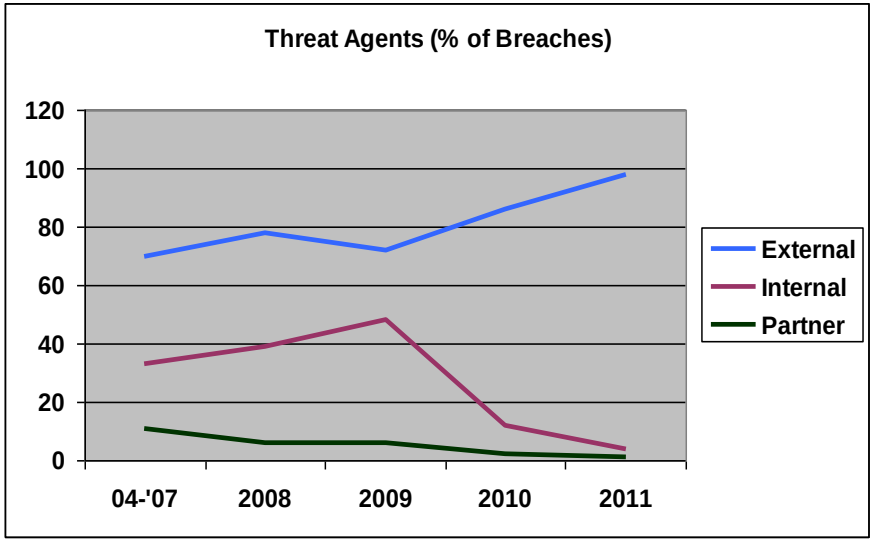


New in 2012:

- 3 new partner/contributors
- Metrics Broken out by Organization Size *(Larger Orgs: >1000 Employees)*
- "Hactivism" increased 25% (100M records)
- PCI & PII stolen in bulk
- IP & SPI stolen in small numbers

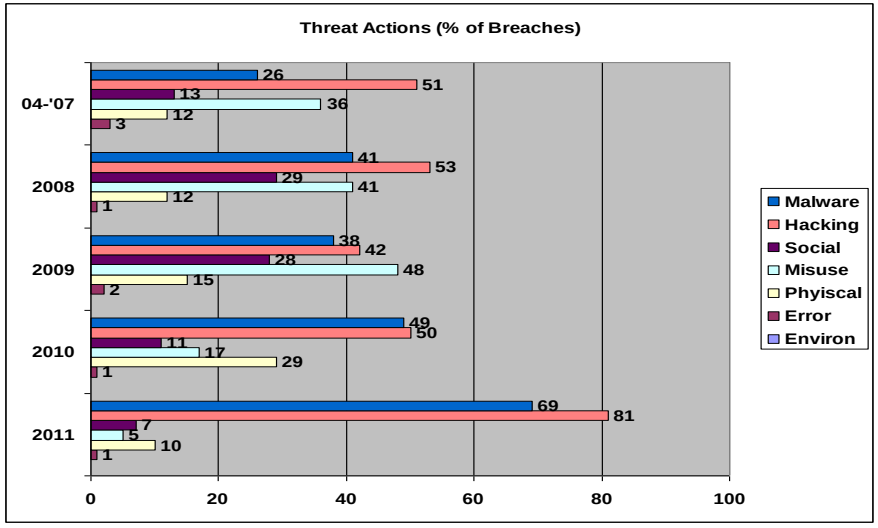


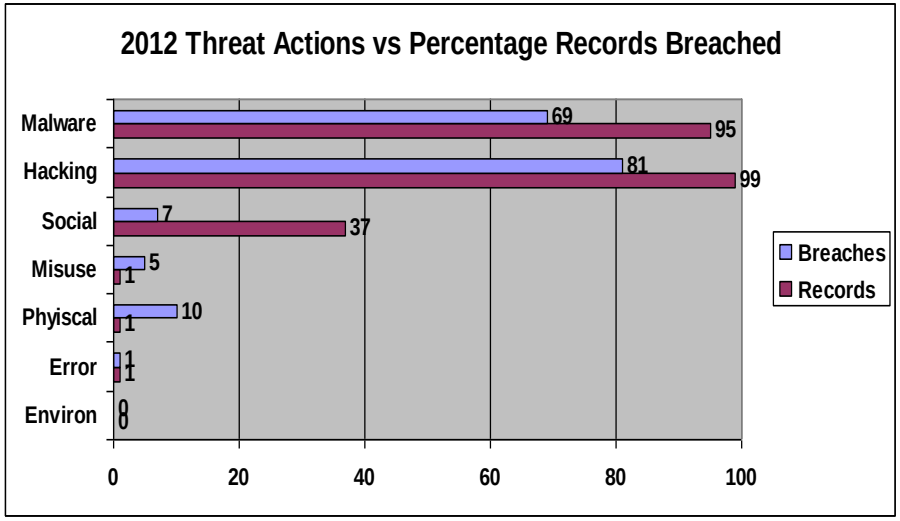
The Threat – Agents and Actions (a second look)



New in 2012 – Con't:

- Malware & Hacking contributed to 95% record compromises
- Stolen Credentials led to 82% records compromised
- Top 3 Compromised Assets (records lost)
  1. Database Server
  2. Web / Application Server
  3. Desktop / Workstation





2011 Verizon Data Breach Investigations Report

Highlights (2010 data – Verizon, USSS and DNHCTF)

Who was Responsible:

92%	External Agents	**(+22%)**
17%	Insiders	(-31%)
<1%	Business Partners	(-10%)
9%	Multiple Parties	(-18%)

Commonalities among breach events

92%	Not considered highly difficult	**(+7%)**
83%	Victims – targets of opportunity	(<>)
76%	Come from server	(-22%)
86%	Discovered by an external party	**(+25%)**
96%	Avoidable with simple controls	(<>)
89%	[PCI loss victims] Not yet PCI compliant	(+10%)

How they did it (methods)

50%	Hacking	(+10%)
49%	Utilized Malware	(+11%)
29%	Physical Attacks	(+14%)
17%	Privileged Misuse	(-31%)
11%	Used Social Eng.	(-17%)

Mitigation Focus Areas:

- Eliminate unnecessary data; Keep track of sensitive data
- Ensure essential [key] controls are met
- Double check the above again
- Assess remote access services
- Test and review web applications
- Audit user accounts and monitor privileged activity
- Monitor [review] and mine event logs

2010 Verizon Data Breach Investigations Report

Highlights (2009 data – Verizon and the USSS)

Who was Responsible:

70%	External Agents	(-9%)
48%	Insiders	(+26%)
11%	Business Partners	(-23%)
27%	Multiple Parties	(-12%)

Commonalities among breach events

98%	Come from servers	(-1%)
85%	Not considered highly difficult	
61%	Discovered by an external party	(-8%)
86%	Breach evident in log files	
96%	Avoidable with simple controls	(+9%)
79%	[PCI loss victims] Not yet PCI compliant	

How they did it (methods)

48%	Privileged Misuse	(+26%)
40%	Hacking	(-24%)
38%	Utilized Malware	(no change)
28%	Used Social Eng.	(+16%)
15%	Physical Attacks	(+6%)

Mitigation Focus Areas:

- Eliminate unnecessary data; Keep track of sensitive data
- Ensure essential [key] controls are met
- Double check the above
- Test and review web applications
- Filter out bound traffic
- Monitor [review] and mine event logs