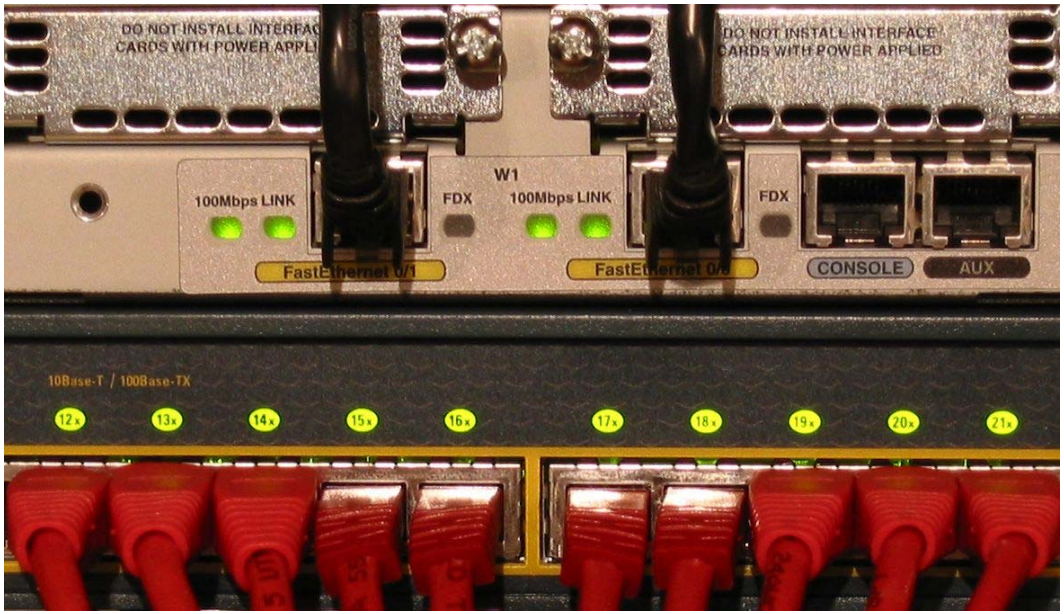
SANS IR and Forensics Summit 2009 Keynote



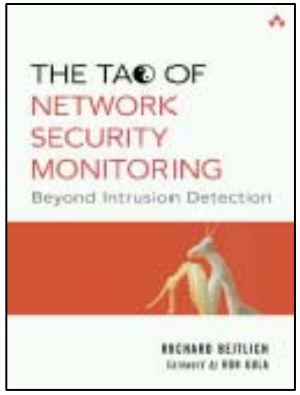
TAOSECURITY

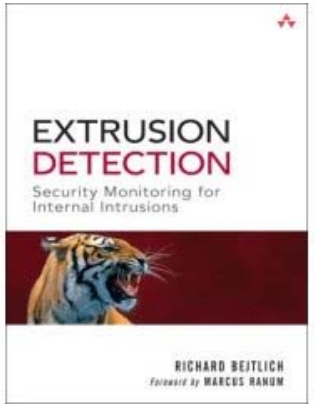
THE WAY OF DIGITAL SECURITY

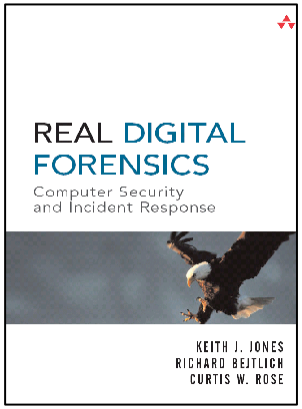
Richard Bejtlich
Director of Incident Response, General Electric
richard@taosecurity.com
taosecurity.blogspot.com

Introduction

- Bejtlich ("bate-lik") biography
  - General Electric, (07-present)
  - TaoSecurity (05-07)
  - ManTech (04-05)
  - Foundstone (02-04)
  - Ball Aerospace (01-02)
  - Captain at US Air Force CERT (98-01)
  - Lt at Air Intelligence Agency (97-98)
- Author
  - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
  - TaoSecurity Blog (http://taosecurity.blogspot.com)







Overview

- Still speaking Truth to Power
- Verizon Data Breach Report
- 7 Stages of Security Team Evolution and Cheap IT
- Defender's vs Intruder's Dilemmas
- Digital Situational Awareness
- Incident Phases of Compromise
- Info Sec Incident Classification

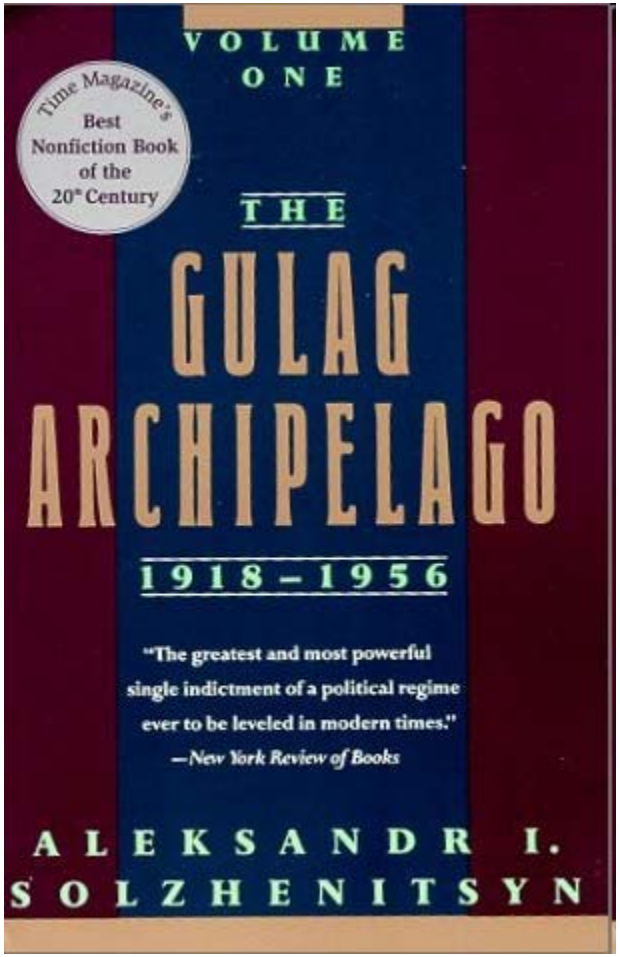
Bring them on! I prefer a straight fight to all this sneaking around.

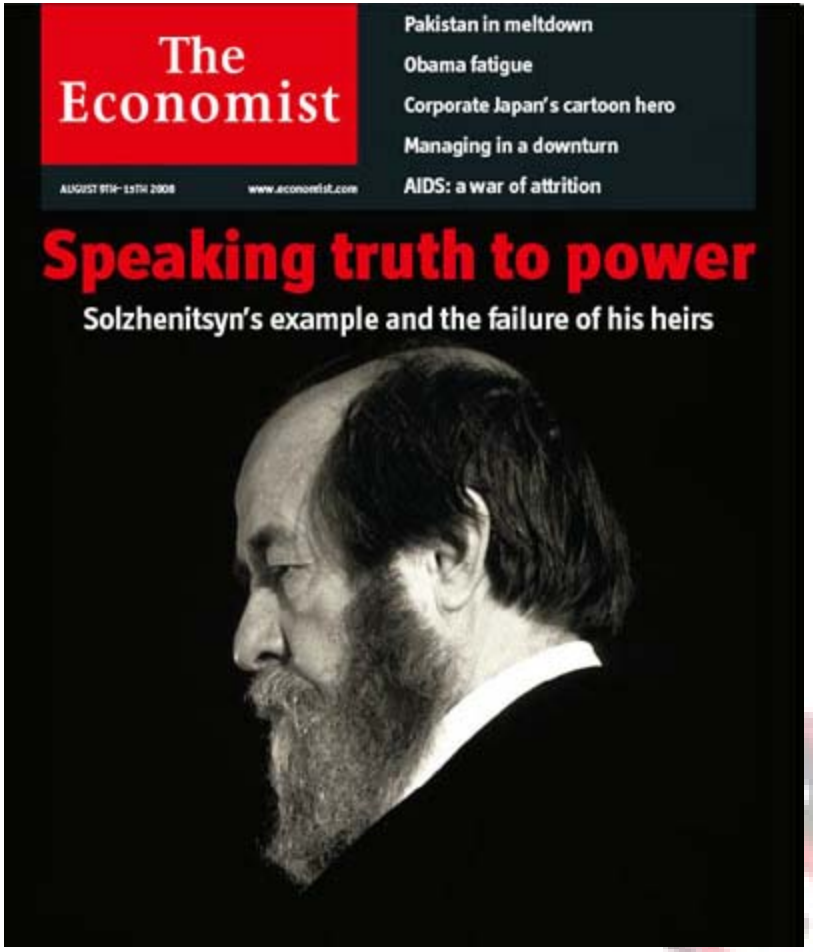
Han Solo, SWEPIV

Still Speaking Truth to Power

- Alexander Solzhenitsyn (1918-2008), author of The Gulag Archipelago: “Don’t lie! Don’t participate in lies! Don’t support a lie!”

Ref: 7 Aug 2008 *Economist* magazine



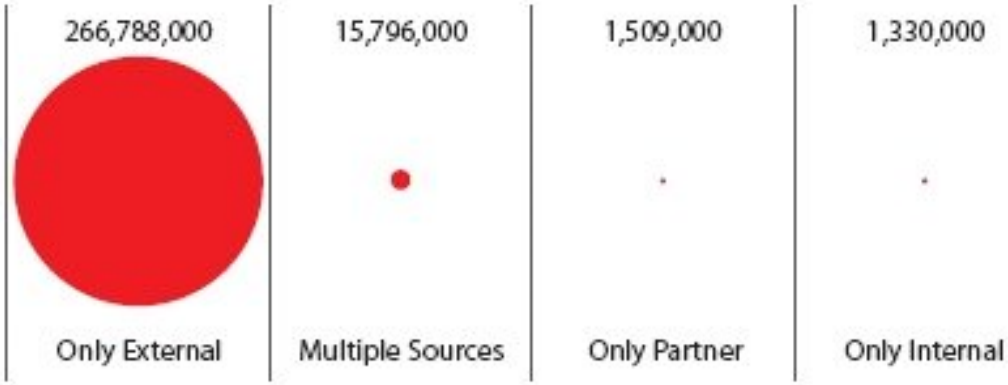


Highlights from 2009 Verizon Data Breach Report 1

Results from 600 incidents over five years make a strong case against the long-abiding and deeply held belief that insiders are behind most breaches.

Who is behind data breaches?	
74% resulted from external sources (+1%).	Closely resembling the stats from our 2008 report, most data breaches continue to originate from external sources. Though still a third of our sample, breaches linked to business partners fell for the first time in years. The median size of breaches caused by insiders is still the highest but the predominance of total records lost was attributed to outsiders. 91 percent of all compromised records were linked to organized criminal groups.
20% were caused by insiders (+2%).	
32% implicated business partners (-7%).	
39% involved multiple parties (+9%).	

Figure 8. Total records compromised by source



Highlights from 2009 Verizon Data Breach Report 2

Figure 6. Breach sources over time by percent of breaches

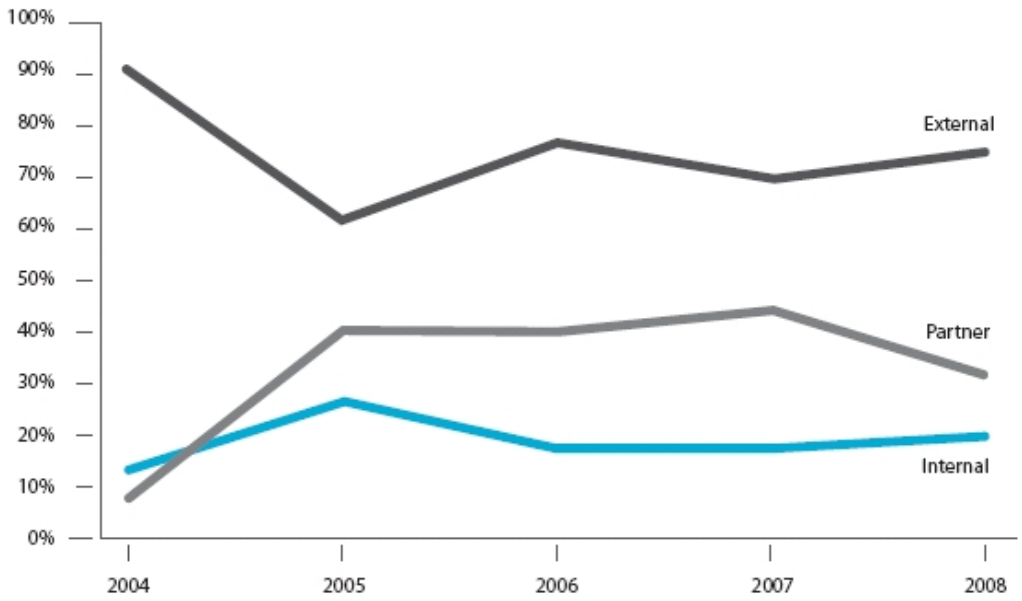


Figure 7. Median number of records compromised per breach

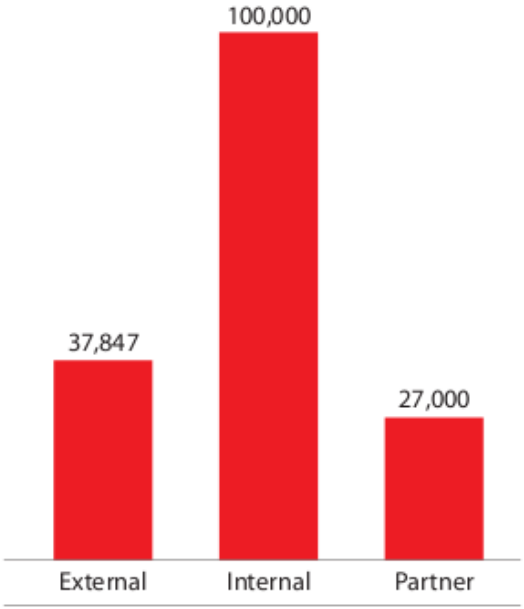
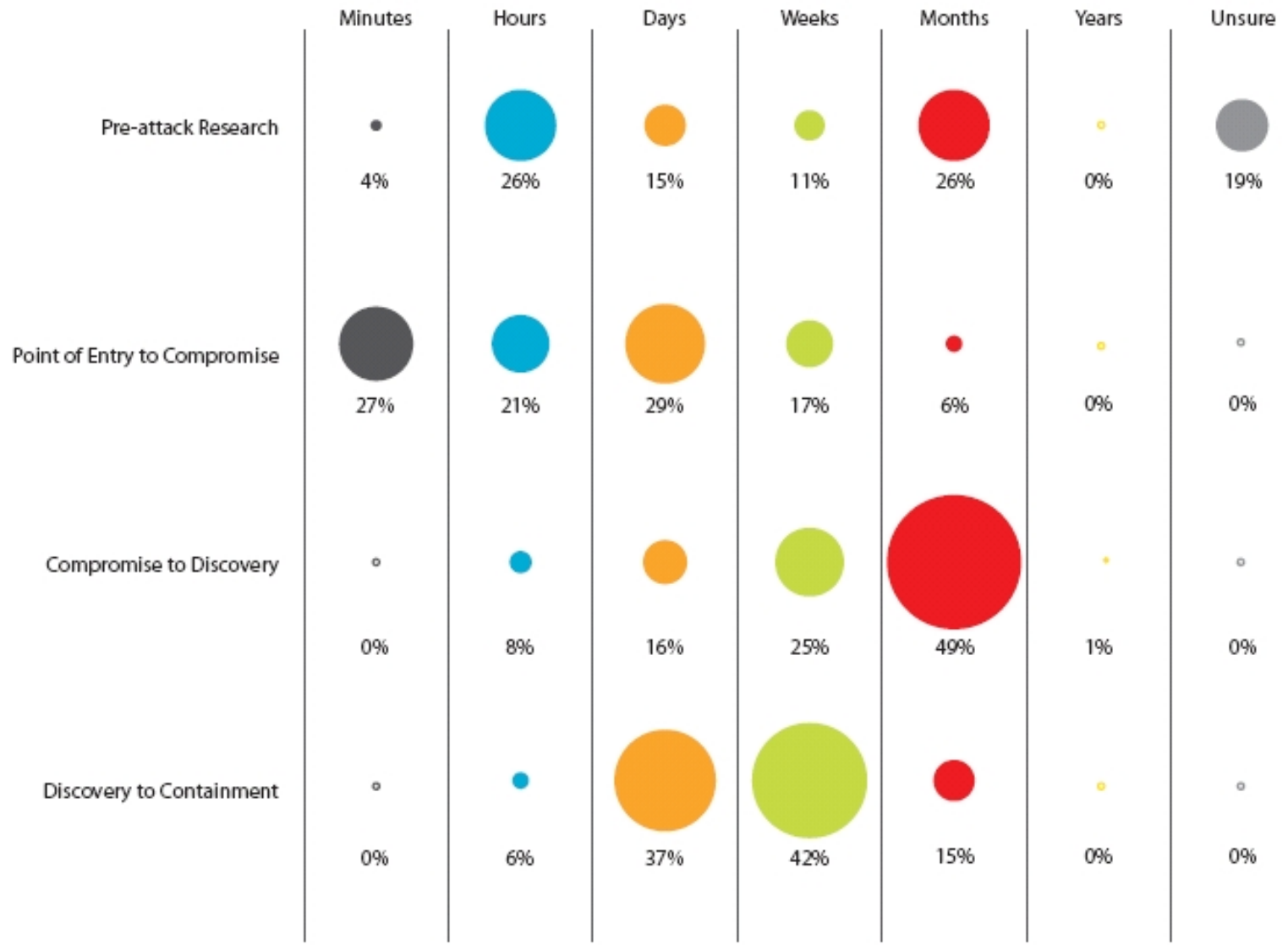


Table 1. Pseudo risk calculation

Source	Likelihood	Impact (number of records)	Risk (pseudo)
External	**74%**	37,847	28,175
Internal	20%	**100,000**	20,000
Partner	32%	27,000	8,700

Highlights from 2009 Verizon Data Breach Report 3

Figure 31. Time span of breach events by percent of breaches



Highlights from 2009 Verizon Data Breach Report 4

Figure 32. Breach discovery methods by percent of breaches

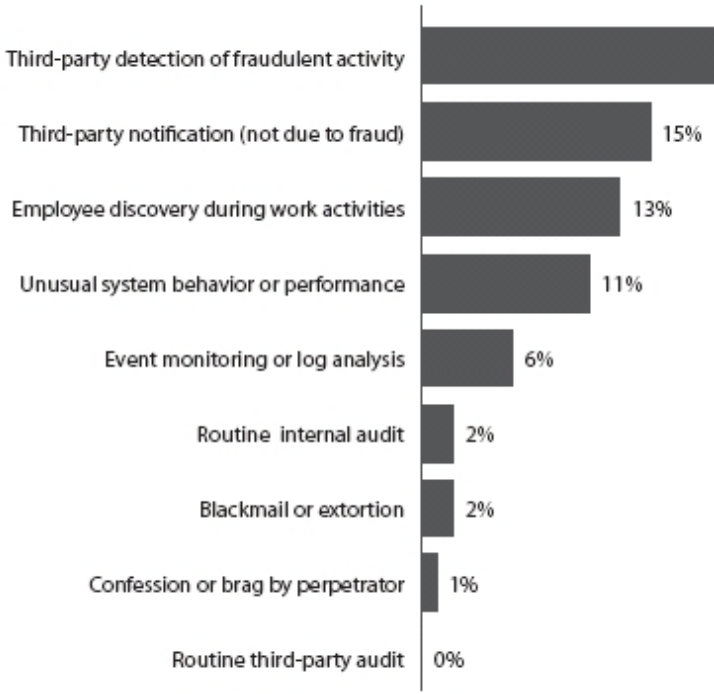
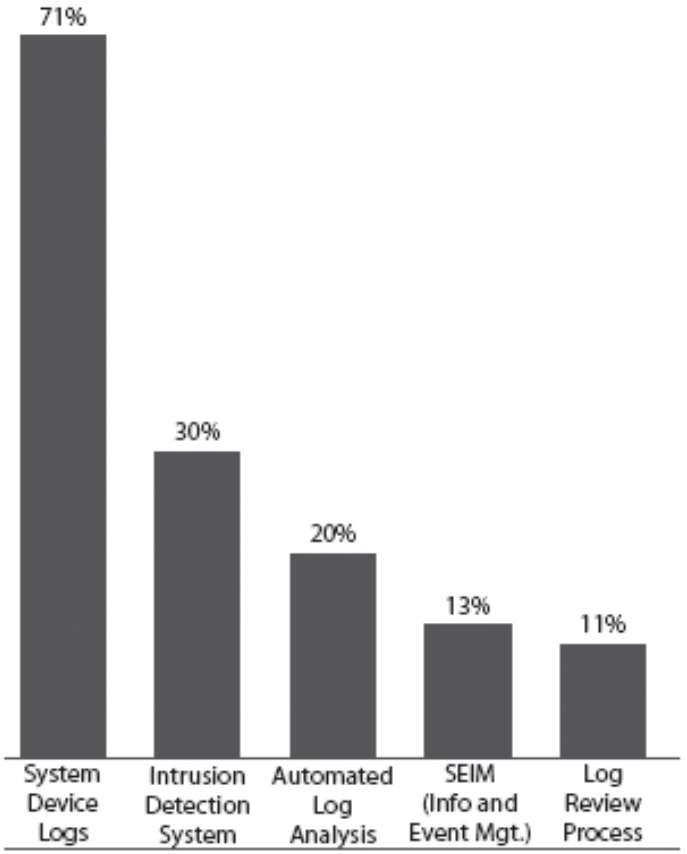


Figure 34. Detective controls by percent of breach victims



Highlights from 2009 Verizon Data Breach Report 5

Figure 35. Incident response practices by percent of breach victims

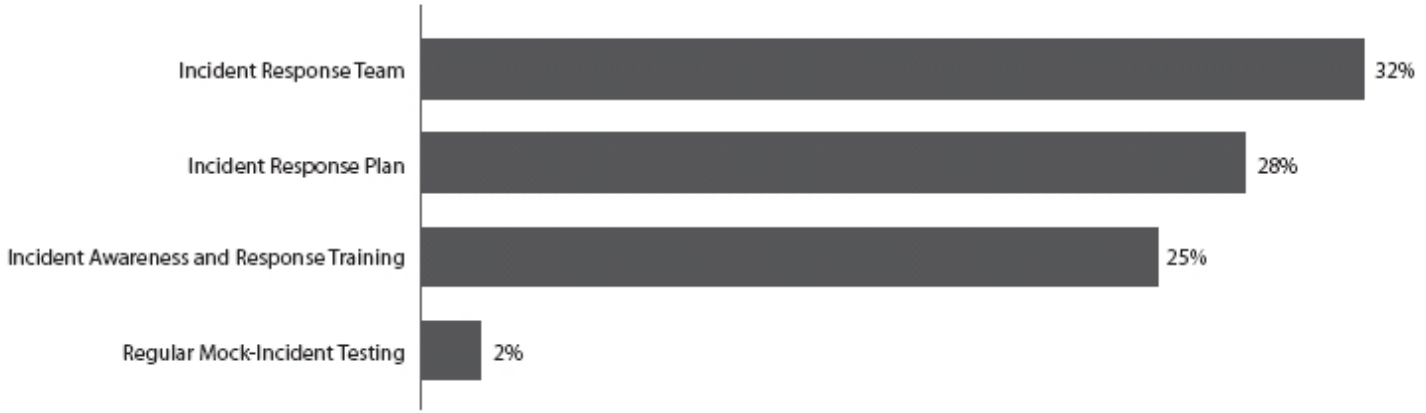
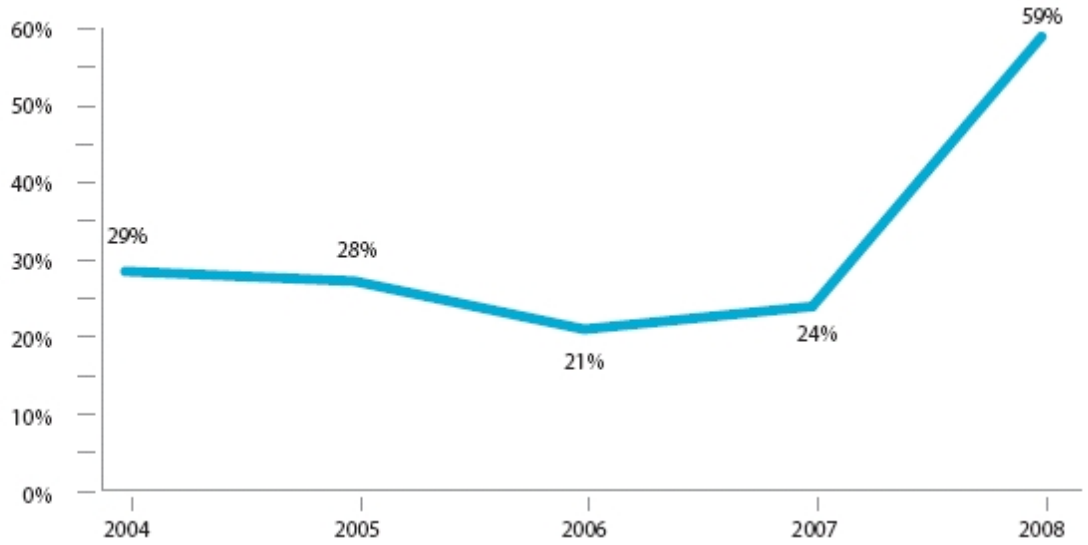
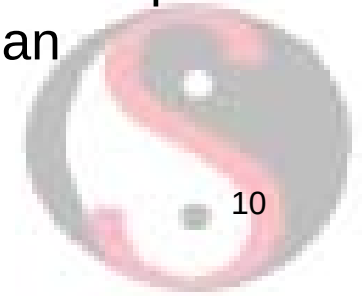


Figure 19. Malware customization by percent of breaches involving malware



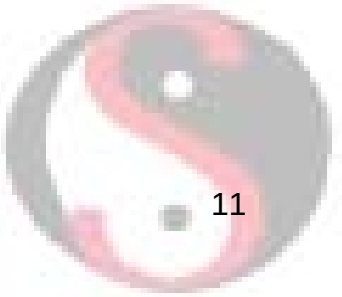
Cheap IT Is Ultimately Expensive

- It is **not cheaper** to run legacy platforms, operating systems, and applications because "updates break things."
- It is **not cheaper** to delay patching because of "business impact."
- It is **not cheaper** to leave compromised systems operating within the enterprise because of the "productivity hit" taken when a system must be interrupted to enable security analysis.
- It is **not cheaper** to try to manually identify and remove individual elements of malware and other persistence mechanisms, rather than rebuild from the ground up (and apply proper updates and configuration improvements to resist future compromise).
- It is **not cheaper** to watch intellectual property escape the enterprise in order to prove that intruders are serious about stealing an organization's data.



7 Stages of Security Team Evolution

1. **Ignorance**. "Security problem? What security problem?"
2. **Denial**. "I hear others have security problems, but we don't."
3. **Incompetence**. "We have to do something!"
4. **Heroics**. "Stand back! I'll fix it!"
5. **Capitalization**. "Now I have some resources to address this problem."
6. **Institutionalization**. "Our organization is integrating our security measures into the overall business operations."
7. **Specialization**. "We're leveraging our unique expertise in X and Y to defend ourselves and contribute back to the security community."



Defender's Dilemma

The intruder only needs to exploit one of the victims in order to compromise the enterprise.

Intruder

Defender

Victims

Intruder's Dilemma

Intruder

The defender only needs to detect one of the indicators of the intruder's presence in order to initiate incident response within the enterprise.

Defender

Victims

OSSEC

Host security monitoring

F-Response

```
D:\binaries\Volatility-1.3_Beta>python volatility -h
Error: Invalid module [-h].

        Volatile Systems Volatility Framework v1.3
        Copyright (C) 2007,2008 Volatile Systems
        Copyright (C) 2007 Komoku, Inc.
        This is free software; see the source for copying conditions.
        There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.

        usage: volatility cmd [cmd_opts]

        Run command cmd with options cmd_opts
        For help on a specific command, run 'volatility cmd --help'
```

Live response and forensic analysis

Security Monitoring

SNORT

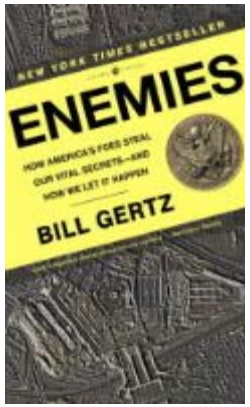
Bro

Network security monitoring

Enterprise log monitoring

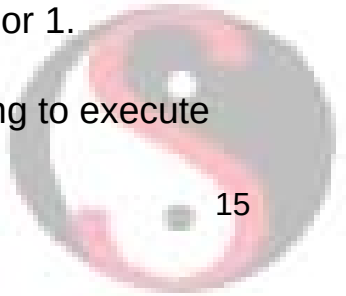
Digital Situational Awareness Methods

- External notification
- Vulnerability assessment
- Adversary simulation or penetration testing
- Incident detection and response (3 paradigms)
  1. Detection is futile.
  2. Sufficient knowledge.
  3. Indicators plus retrospective security analysis.
- Counterintelligence operations
  - See who is selling or offering to sell your information or access to your information.
  - Solicit the underground for your organization's data or for access to your organization.
  - Penetrate adversary infrastructure.
  - Infiltrate the adversary group.
  - Pose as an individual underground member.



Incident Phases of Compromise

- Reconnaissance. Identify target assets and vulnerabilities, indirectly or directly. Cat 6.
- Exploitation. Abuse, subvert, or break a system by attacking vulnerabilities or exposures. If the intruder does not seek to maintain persistence, then this could be the end of the compromise. Cat 2 or 1.
- Reinforcement. The intruder deploys his persistence and stealth techniques to the target. Still Cat 2 or 1, leading to Breach 3.
- Consolidation. The intruder ensures continued access to the target by establishing remote command-and-control. Breach 3.
- Pillage. The intruder executes his mission. Here we assume data theft and persistence are the goals.
  - Propagation. Intruders usually expand their influence before stealing data, but this is not strictly necessary. At this point the incident classifications should be applied to the new victims.
  - Exfiltration. The intruder steals data. Depending on the type of data, Breach 2 or 1.
  - Maintenance. The intruder ensures continued access to the victim until deciding to execute another mission.



Information Security Incident Classification

Information Security Incident Classification for Individual System Compromise

Richard Bejtlich 05 June 2009

Classification	Number	Color	Description
Vuln 3	1		Intruder must apply substantial effort to compromise asset and exfiltrate sensitive data
Vuln 2	2		Intruder must apply moderate effort to compromise asset and exfiltrate sensitive data
Vuln 1	3		Intruder must apply little effort to compromise asset and exfiltrate sensitive data
Cat 6	4		Intruder is conducting reconnaissance against asset with access to sensitive data
Cat 3	5		Intruder is attempting to exploit asset with access to sensitive data
Cat 2	6		Intruder has compromised asset with access to sensitive data but requires privilege escalation
Cat 1	7		Intruder has compromised asset with ready access to sensitive data
Breach 3	8		Intruder has established command and control channel from asset with ready access to sensitive data
Breach 2	9		Intruder has exfiltrated nonsensitive data or credentials/access techniques that will facilitate access to sensitive data
Breach 1	10		Intruder has exfiltrated sensitive data or is suspected of exfiltrating sensitive data based on volume, etc.

Note: Traditional incident response teams use events of impact 6 or higher to denote true "incidents," i.e., compromise of an asset.

Crisis 3. 11 / Intruder has publicized data loss via online or mainstream media.

Crisis 2. 12 / Data loss prompts government or regulatory investigation with fines or other legal consequences.

Crisis 1. 13 / Data loss results in physical harm or loss of life.

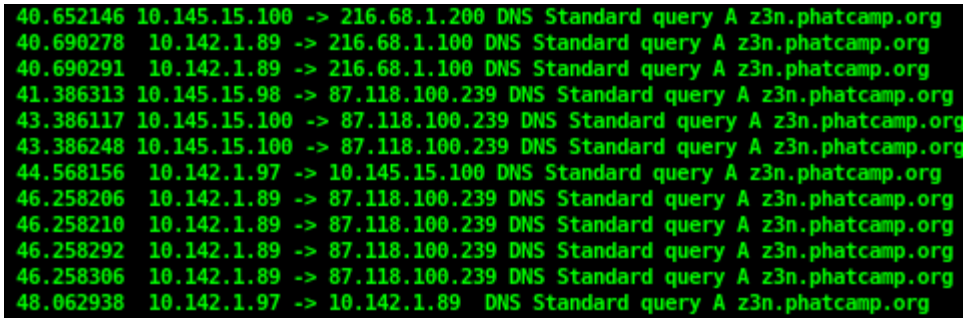
Crisis 0. 14 / Organization ceases to exist.

References

- http://taosecurity.blogspot.com/2009/05/lessons-from-cdx.html
- http://taosecurity.blogspot.com/2009/05/highlights-from-2009-verizon-data.html
- http://taosecurity.blogspot.com/2009/05/cheap-it-is-ultimately-expensive.html
- http://taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html
- http://taosecurity.blogspot.com/2009/06/information-security-incident.html
- http://taosecurity.blogspot.com/2009/06/incident-detection-paradigms.html
- http://taosecurity.blogspot.com/2009/06/incident-phases-of-compromise.html

Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES



Richard Bejtlich

richard@taosecurity.com

taosecurity.blogspot.com