Using Security Intelligence to Stay out of the Headlines

Chris Poulin

IBM, Security Systems

Session ID: DAS-309

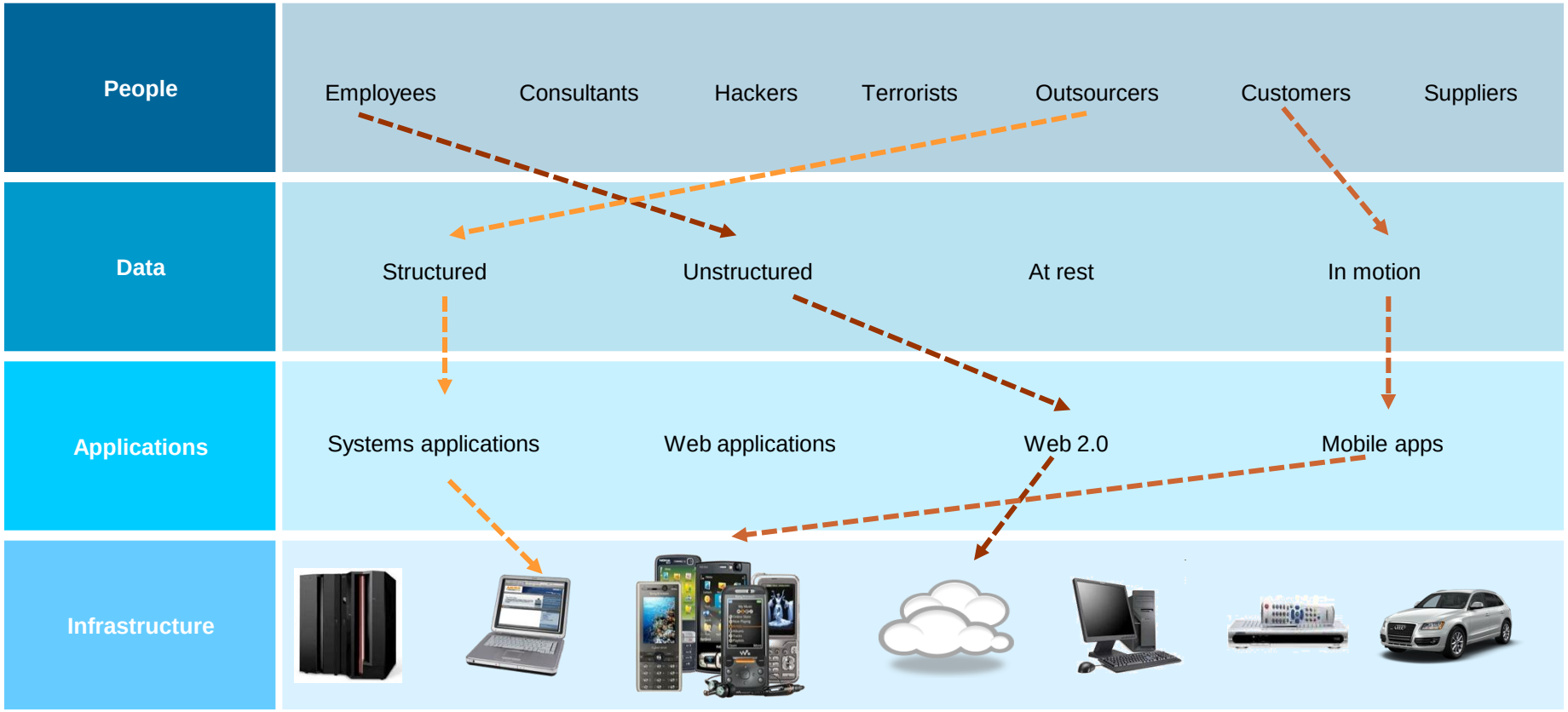
Session Classification: Intermediate

Welcome to the SIEM Crime Scene

- Remove yourself from the RSA event & help me solve the case of Security Intelligence

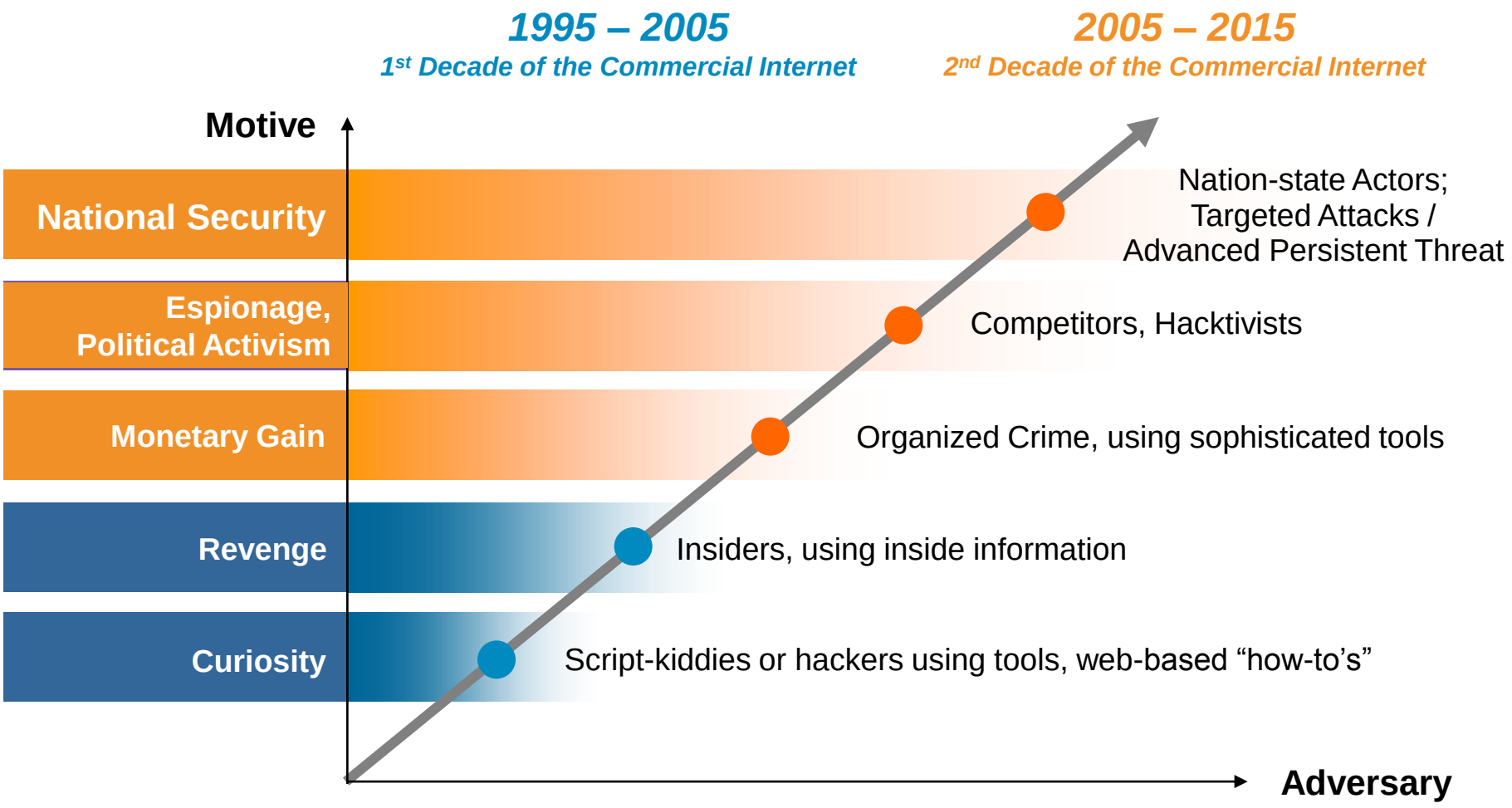
- I will be presenting to you:
  - The facts
  - The criminals & targets
  - Food: recipe for success

Technology is more complicated

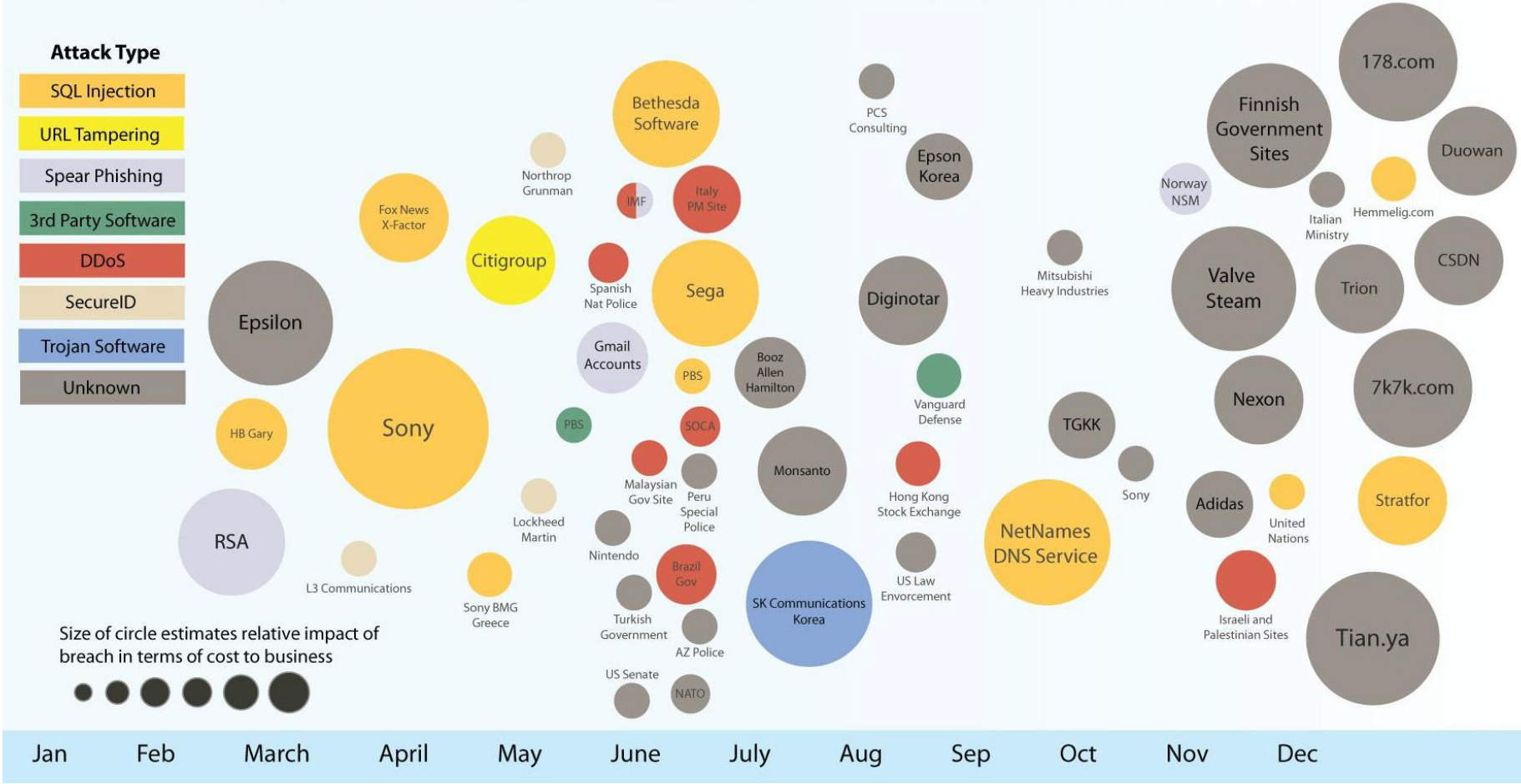


It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

Attackers & motives are more sophisticated

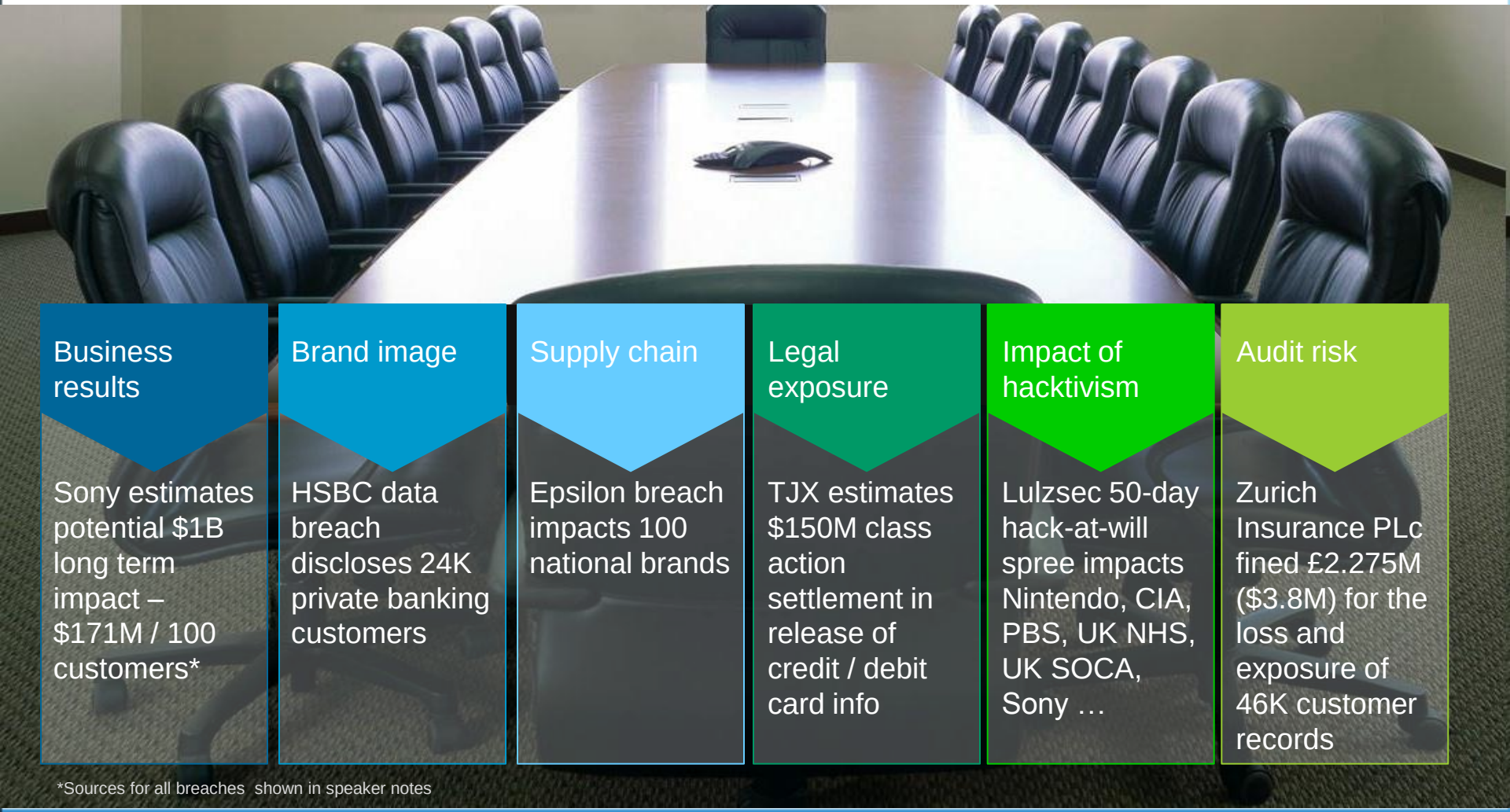


Targeted attacks in the headlines



IBM Security X-Force® 2011 Trend and Risk Report

Security threats affect the business

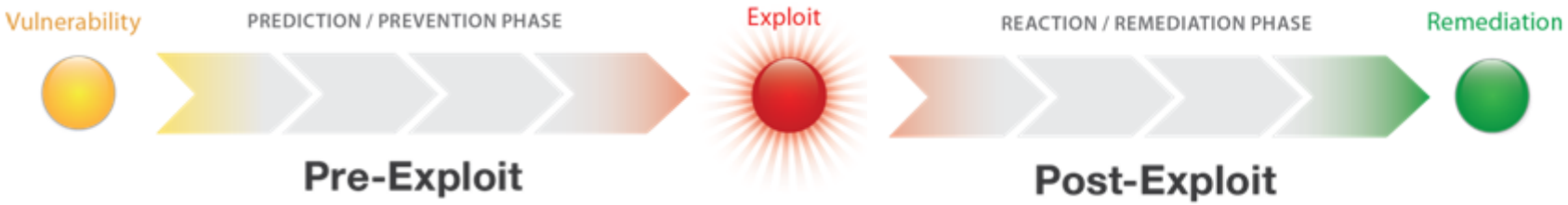


Business results	Brand image	Supply chain	Legal exposure	Impact of hacktivism	Audit risk
Sony estimates potential $1B long term impact – $171M / 100 customers*	HSBC data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates $150M class action settlement in release of credit / debit card info	Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …	Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

*Sources for all breaches shown in speaker notes

Security Intelligence

Security Intelligence Timeline



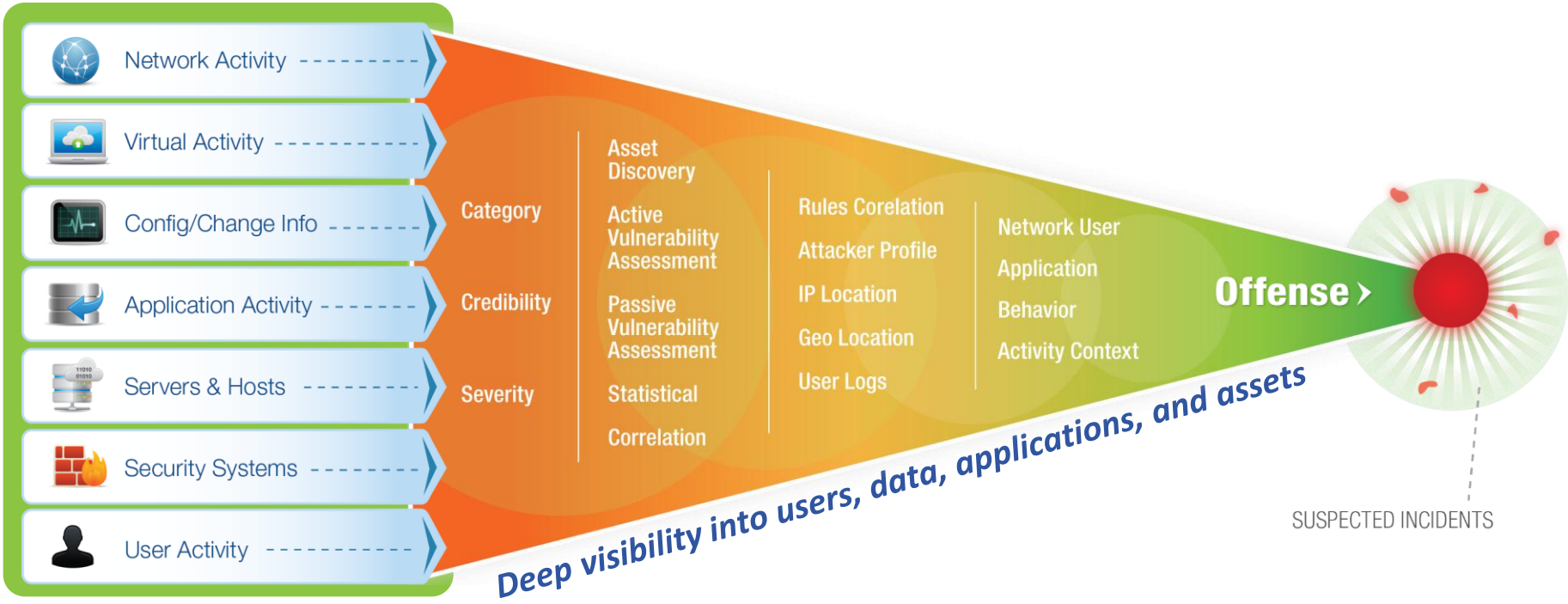
Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

Collect, normalize, apply context & correlate



Sources + Intelligence = Accurate & Actionable Insight

Security Intelligence Case Studies

Cascading security failures: Worst case

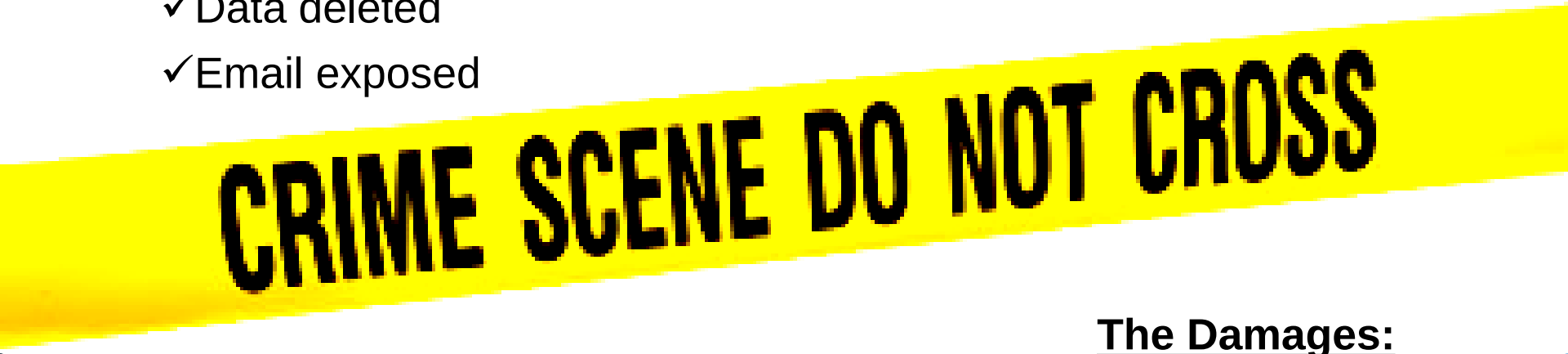
The Crime:

✓Website defaced

✓Intellectual property stolen

✓Data deleted

✓Email exposed



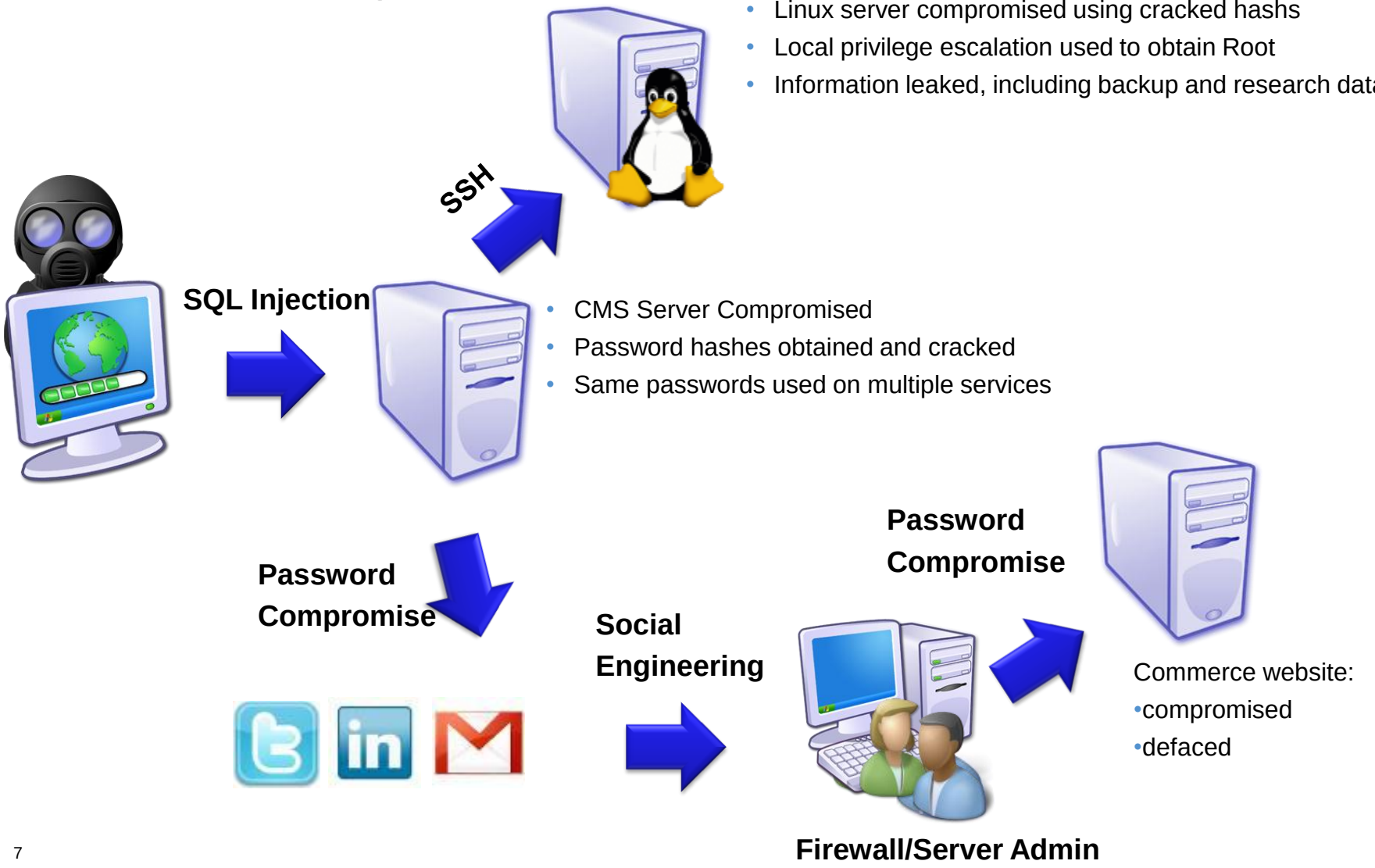
The Damages:

Business reputation damage

IP loss—incalculable

Recovery costs

The Investigation



- Linux server compromised using cracked hashs
- Local privilege escalation used to obtain Root
- Information leaked, including backup and research data

- CMS Server Compromised
- Password hashes obtained and cracked
- Same passwords used on multiple services

The Sentence

- Arrest of 4 in the US and UK
- 1 indicted but not arrested in Ireland
- CEO of the victim company stepped down
- The company subsequently sold its assets

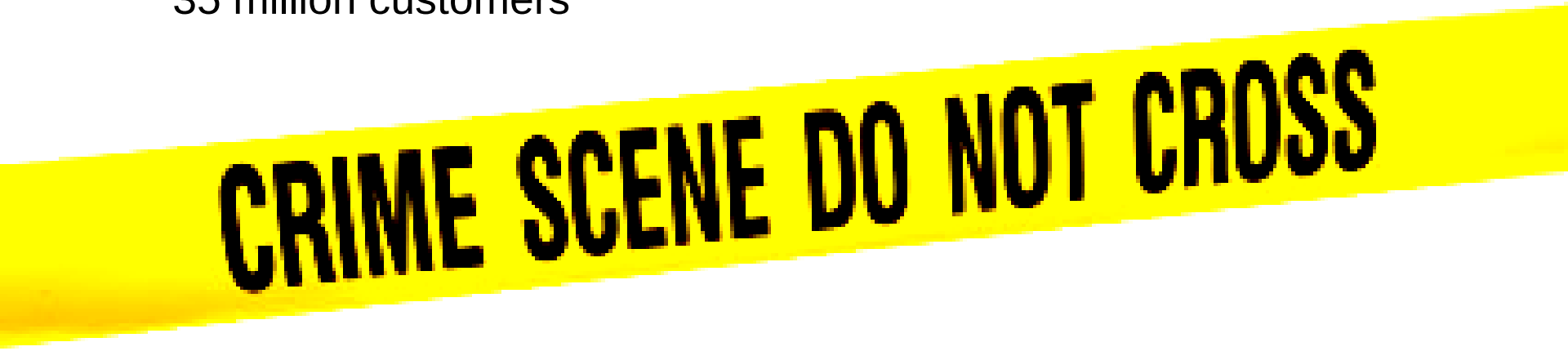
Lesson learned: take care of the basics

- Patch & protect public-facing resources
- Password strength & policy (re-use)
- Eat your own dog food

Anatomy of an APT

The Crime:

✓Theft of personal details of 35 million customers



The Damages:

Cost estimates ~2B USD

The Investigation

3rd Party Software Update Server Compromised

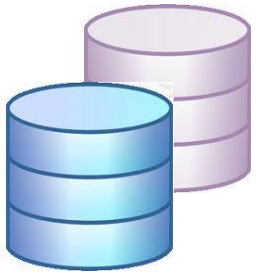
Attackers create Trojan

Trojan “auto-updated” to Corporate network

Port 8080 used for C&C activities

35M records stolen

60+ Corporate computers infected w/ backdoor agent



–6 Months Day 0 Day 8

The Sentence

- No arrests have been made
- China was (once again) implicated

Lessons learned:

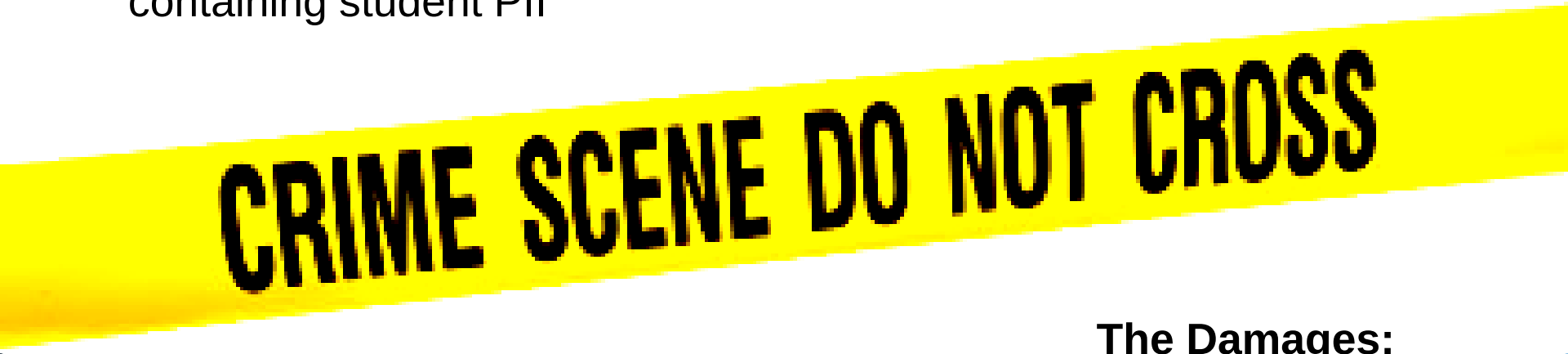
- Even with a strong security program…
- …and it can work against you
- Log & monitor

A tale of two universities

The Crime:

✓Two universities

✓Both detect compromise of system containing student PII



The Damages:

Differ greatly between the two organizations…

The Investigation

University A: with Security Intelligence

- Analysis of network data to/from compromised
- Copyrighted material only, not student PII
- Host cleaned and no one outside notified

University B: No SIEM / Log Management

- No content & flow analysis;
- Can’t be ascertained which (if any) data stolen
- Notify ALL students of the **potential** loss of privacy;
- Setup a call center to answer questions
- Lots of ~~€€€~~ / ~~£££~~ / $$$, bad PR

The Sentence

- Uni A: Attacker was identified as external;
  no student was involved (though they had used security intelligence many time to catch insiders)
- Uni B: No one was caught

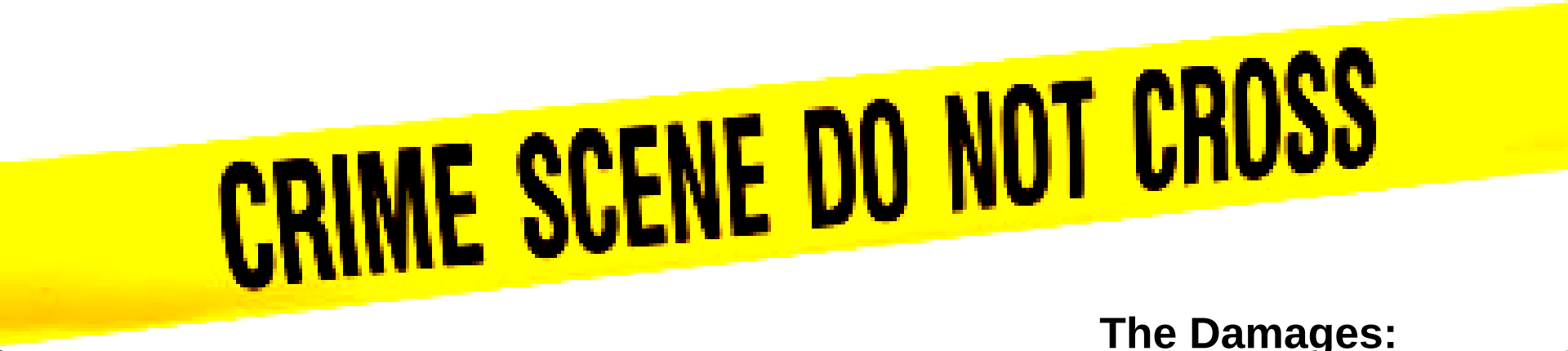
Lessons learned:

- Central logging is critical
- Network activity with DPI is critical
- Pay €/£ now or ~~€€€€€~~/~~£££££~~ later

A/V without signatures

The Crime:

✓Virus infection



The Damages:

Minimal:
detected before it spread

The Investigation

Energy/Utility Company

- Detected “Here You Have” virus
- Two A/V products: no signature yet
- Network behaviour analytics auto-alert

Infrastructure Solutions Provider

- Remote employees laptop
  attacking network across VPN
- User behaviour analytics alert: unusual network traffic
- Automatic alert to security team

The Sentence

- Identified user quickly, quarantined computer
- Determined employee's child used his computer for games

Lessons learned:

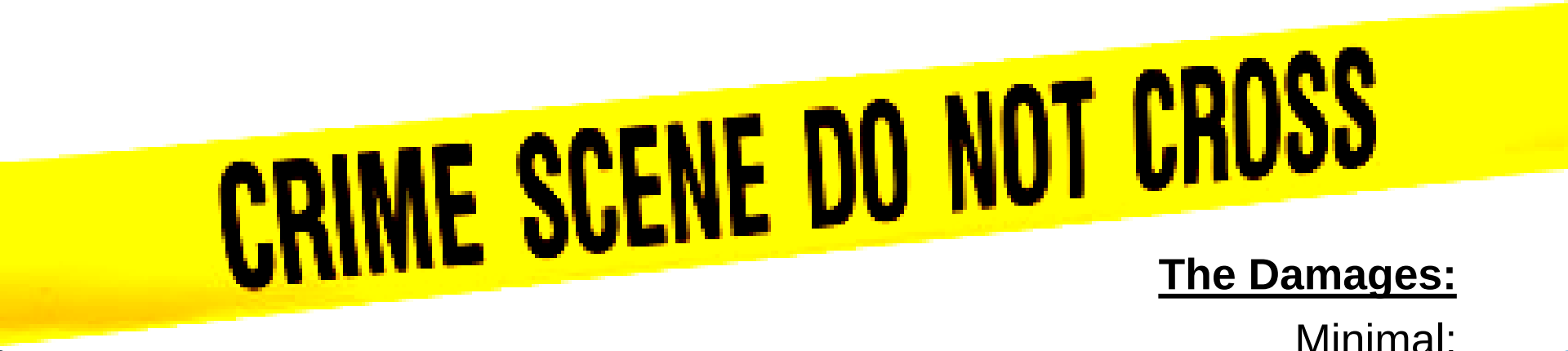
- Behavioural analytics provide early warning
- Both network activity and event monitoring
- A/V by itself is not enough

Financial Fraud

The Crime:

✓Consumer credit fraud

✓Financial fraud



The Damages:

Minimal:

Perpetrators detected before the crime is committed

The Investigation

Consumer Credit Agency

- Collect events from web site and specialized apps
- Baseline behaviour and alert on anomalies
- e.g., car dealership norm = 40 credit queries/day; suddenly starts hitting 70 or more

Financial Trading Company

- Collect events from trading app
- Baseline average # transactions and €/£/$s per
- Alert on deviations

The Sentence

- None: potential fraudsters are stopped before they commit their crime

Lessons learned:

- Stay ahead of the criminals
- Security Intelligence automates baselining normal activity & detecting anomalies
- Bespoke / all applications must be supported
- Behaviour anomaly detection is for both applications and network activity

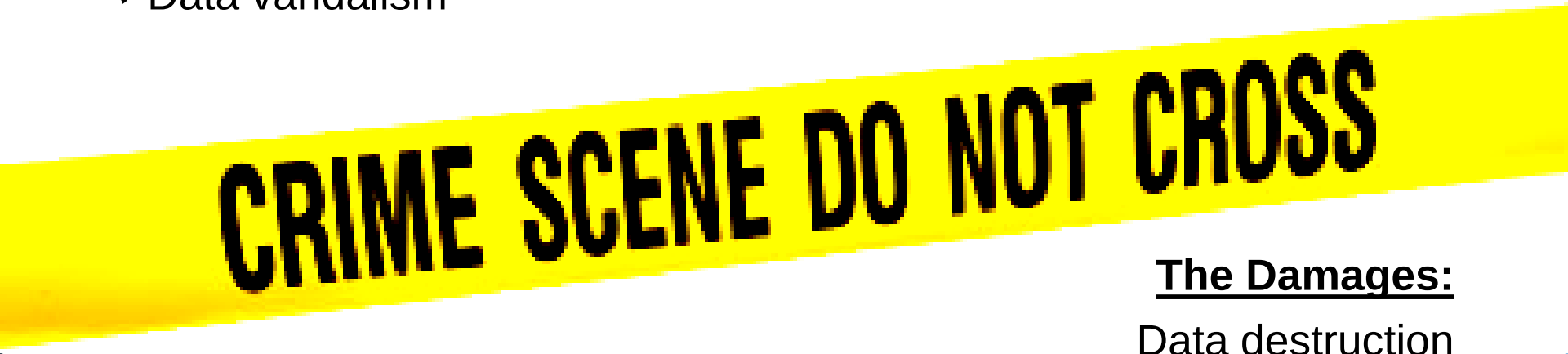
Court-Admissible Forensics

The Crime:

✓Creating backdoor account

✓Breaking into former employer's network

✓Data vandalism



The Damages:

Data destruction

Data recovery costs

Investigation costs

Litigation costs

= $200,000

The Investigation

- Employee was let go (sacked)
- Social engineered creation of rogue account
- Deleted all the files on an email server;
  tried to delete all files on a SAN
- Used Security Intelligence to investigate the incident
  - Correlated events to identify the perpetrator, and
  - Detail his activities
- Information used by the Crown Prosecutor (DA) in court

The Sentence

- Defendant pled guilty on the eve of his trial
- Evidence presumed a major factor in the plea
- Sentencing pending: likely 2 – 6 years

Lessons learned:

- Security Intelligence provides complete forensics
- Precedent for use in legal proceedings

Operationalizing Security Intelligence

Security Intelligence: Recipe for Success

1. Take stock of your assets
2. Grocery shop
3. Mise en place
4. Sauté and stir
5. Simmer
6. Salt to taste

1. Take stock of your assets

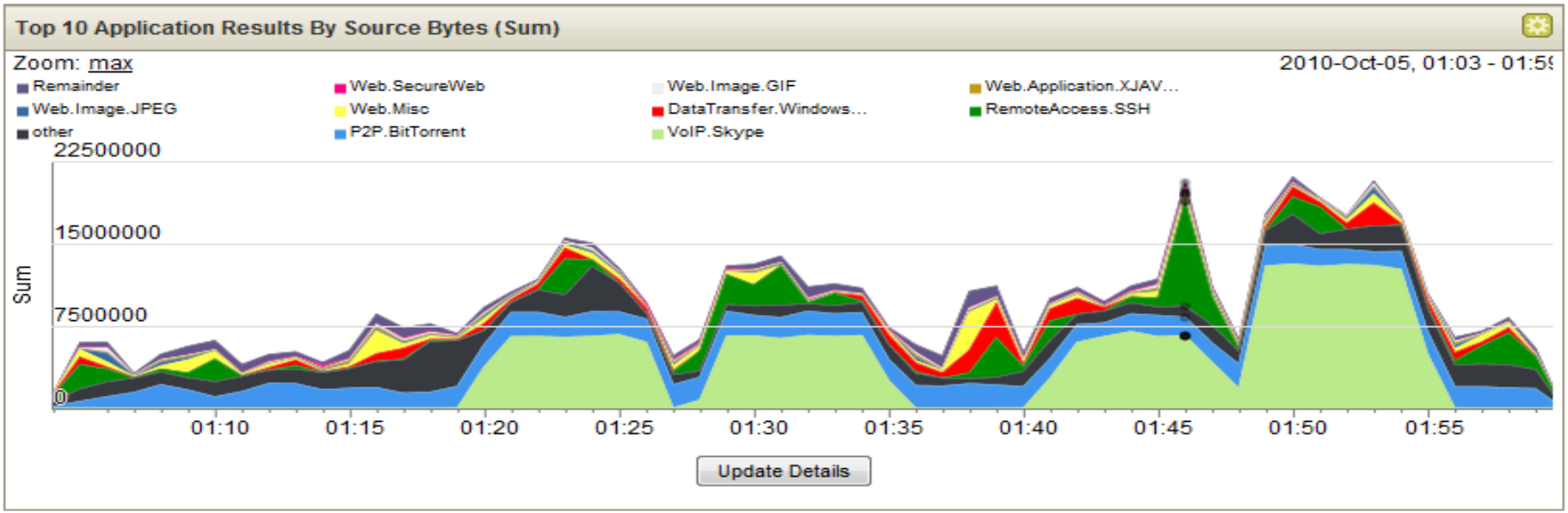
- Enumerate and classify assets & data
- Determine
  - System and application owners
  - Business purpose
  - Authorized roles & users
  - Configuration baselines
  - Change control process
- Review
  - Security policy, standards, & procedures

What are your assets?

- Security Infrastructure:
  - Firewalls, VPN Gateways, switches/routers
  - IPSes, DLP
  - Endpoint security, A/V, DAM, FIM
- Server & Application Logs: Stock and bespoke
- Users: Identity & Access
- Vulnerability & Configuration
- Network activity
- Physical & Virtual infrastructure
- External feeds:
  - Blacklisted sites/IPs, geolocation, IP/application reputation

How to take stock of your assets

- Risk assessment
- Profile environment & assets automatically
  - Passive network monitoring
  - Vulnerability scanning
- Map environment manually



2. Shop: Acquire Technology

- Assess existing collection technology
  - Log management, SIEM, IPS, IAM, etc.
  - Current vs desired state
  - Gap, prioritized by need
- Research vendors or open source
- RFI, RFQ, bake-off, PoC
- TCO, including staffing & maintenance fees
  - Deployment: in-house, consultant, vendor
  - Management—rules, database maintenance, etc
  - Security operations

3. Mise en Place: Plan & Prepare

- Marshal resources, coordinate activities
  - Buy-in from management, system & app owners
  - Schedule of collection activities
  - Corpus of reports and rules
  - Define roles & users
  - Cross-organizational communication & escalation
- Integration with Security Operations
  - People: staffing
  - Process: investigation, coordination, feedback loop
  - Technology: integration w/ticketing system, etc.

4. Sauté & stir: Collection & basic tuning

- Install & configure collectors
  - Network monitoring
  - Event collection
- Configure collection
  - Standard log sources, push & pull
  - Bespoke log sources
- Enable stock/vendor rules – generalized threats
- Basic tuning
  - Tweak rule settings
  - White noise & false positive reduction

5. Simmer: The acclimation period

- Regularly work with Security Intelligence
  - Continuous tuning
  - Review top applications/protocols, top talkers, etc
  - Visualize activity patterns
  - Identify and add new telemetry
  - Investigate suspicious activity and anomalies
- Become proficient with the tools
- Become one with your environment

6. Salt to taste: Custom use cases

- Now that you've achieved SI maturity…
- Start thinking about ways SI can support business requirements
- What is the business requirement?
- How can Security Intelligence satisfy the req?
- What are the sources of telemetry needed?
- Process for investigation / escalation?
- Remember 80/20 rule

Apply slide

- Take stock of your assets
- List out security use cases
- Configure appropriate logging, if only locally
- Assess existing log management and SIEM capability & planned/future requirements
- Avoid analysis paralysis:
  doesn't have to be perfect from the start