The IPO of the 0day

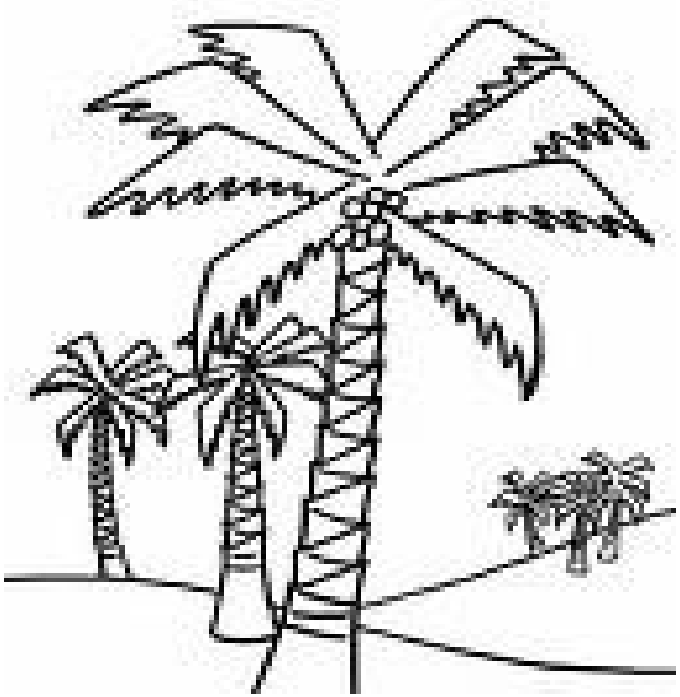
Stock fluctuation from an unrecognized influence.

0day

Understand it, address it, and integrate it.

Background: Justine Aitel, CEO Immunity

- Bloomberg LP, Global CSO
  - ISS XForce
    - GCSB (New Zealand's NSA)



Immunity, founded in 2002, is headquartered in the heart of South Beach, Miami.

IMMUNITY

Taking Control

"Do you know anyone that can do that?"

Influencing Change

1. Getting the face time (power of the demo!)
2. Spending on security is a medium-term investment
3. Re-focus on operations

Note: leave scare tactics to the security vendors!

Welcome to the New World of 0day

Agenda:

- Trading and financial analysis systems are proprietary and have very limited distribution
- Enterprise software such as this is RAMPANT with 0day
- Re-organizing security management in the financial sector
- Management acceptance of the existence of 0day
- Throwing out the IDS
- Less reliance on technology, more reliance on people
- Hiring hackers

0day doesn't mean 0verflow

“The user can't change the network data, it's encrypted.”

The changing definitions of 0day

A bug that

has not been patched,

and is not public.

Alternative definitions are often weaker - they usually benefit the associated line of business.

Who finds 0day, why, and where are they found?

Who:

Traditionally limited to hackers and govt employees, corporations and universities are now in on it too.

Why:

- intellectual (and artistic) self-development
- fame
- $

Where:

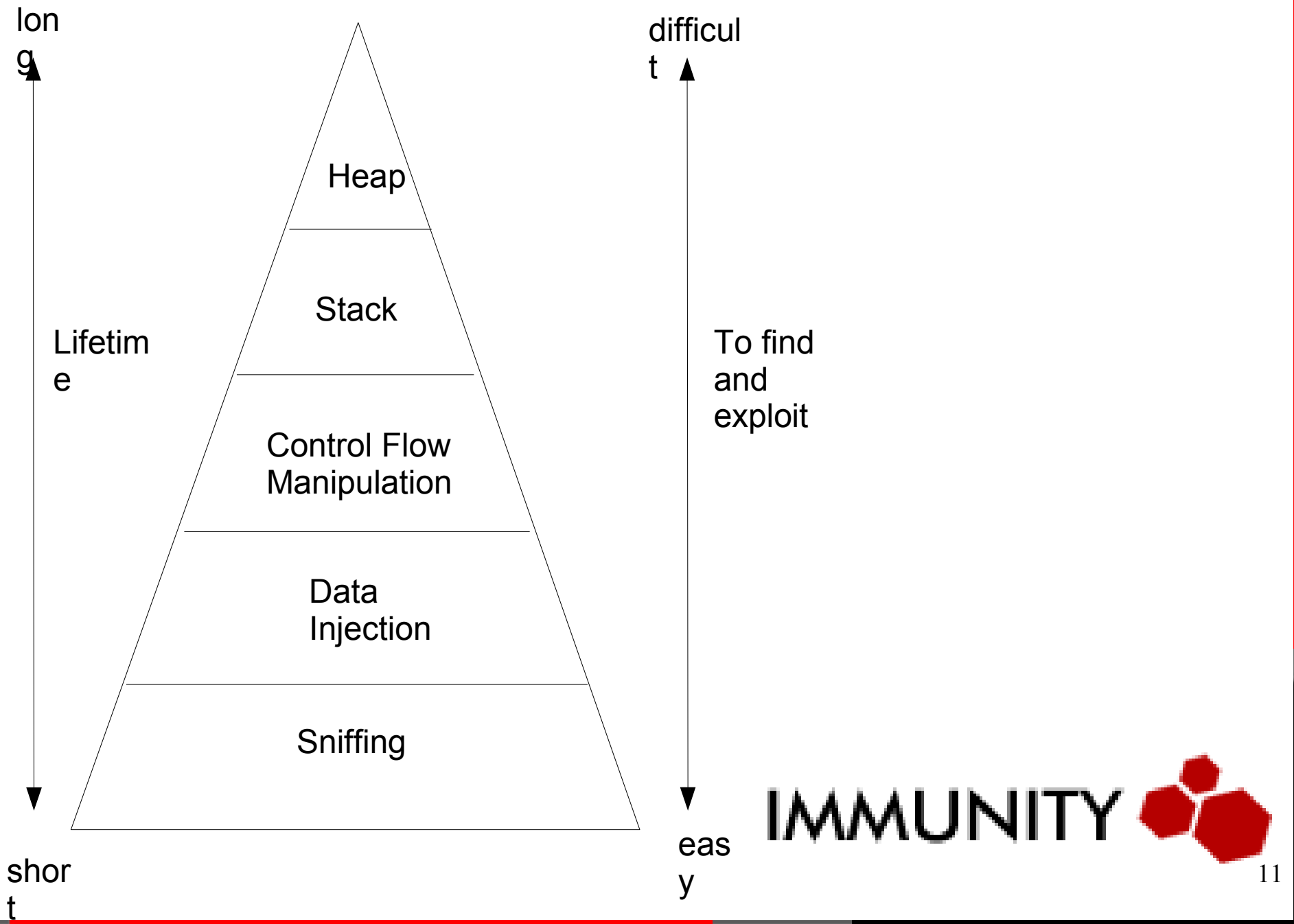
Networked applications, preferably Internet-facing. Now that server vulnerabilities are getting more and more rare, client-sides are gaining value.

How we value 0day

Four contributing factors:

1. Lifespan
2. Uniqueness
3. Relevance
4. Exploitability

0day Value #1: Lifespan



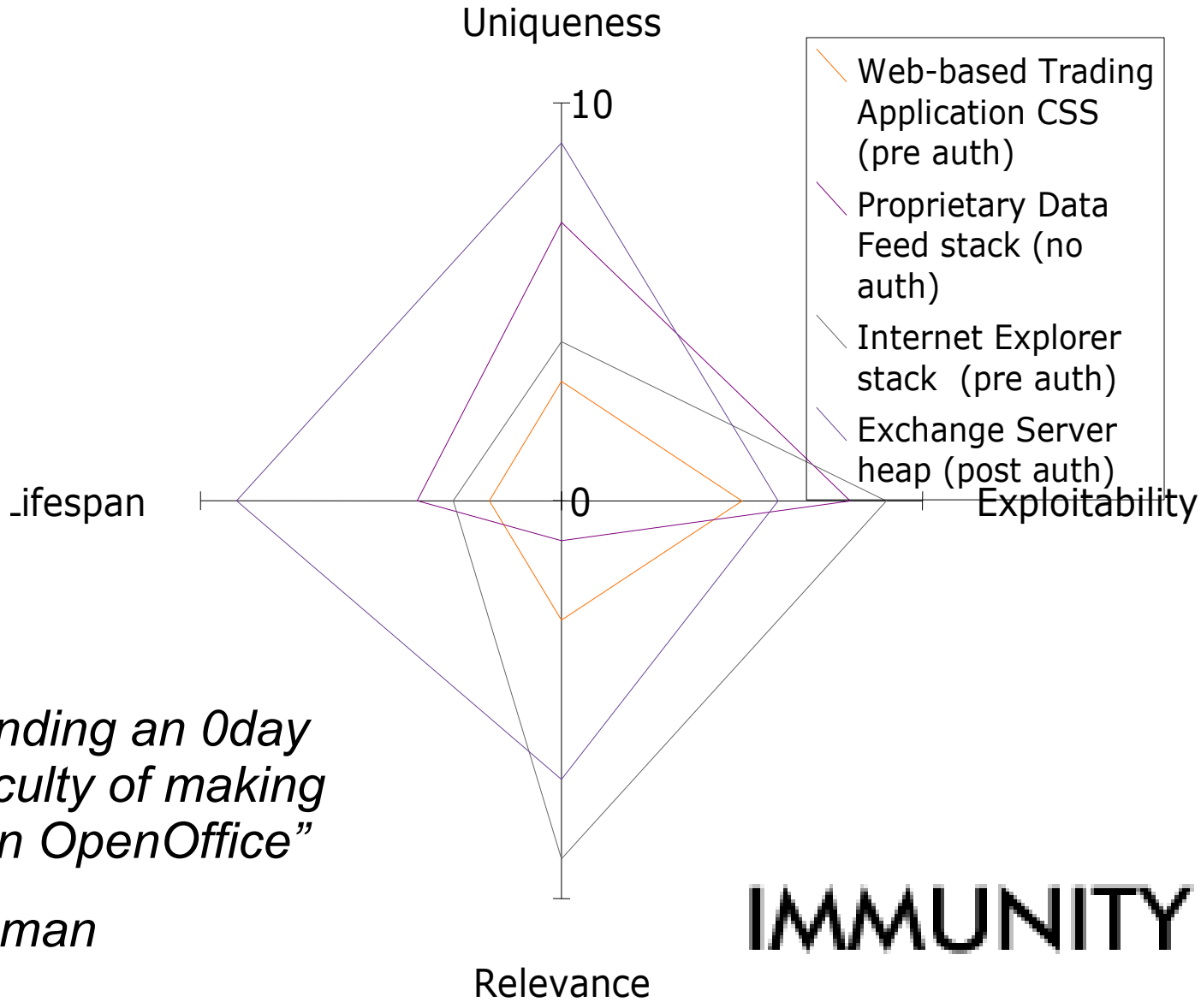
IMMUNITY

Valuing 0day: Factors 2-4

1. Lifetime
2. Uniqueness
   - the prevalence of other similar 0day in same software
3. Relevance
   - coverage, how widely deployed the software is, likely presence of vulnerable systems
4. Exploitability
   - how reliably the exploit will execute

Valuing 0day: Reviewing the Factors

Rate each factor 1 -10 (low-high):



"Difficulty of finding an 0day versus difficulty of making this graph in OpenOffice"

-Nicolas Waisman

IMMUNITY

Real-world 0day Statistics

As of June 16 2007:

Average 0day lifetime: 348 days

Shortest life: 99 days

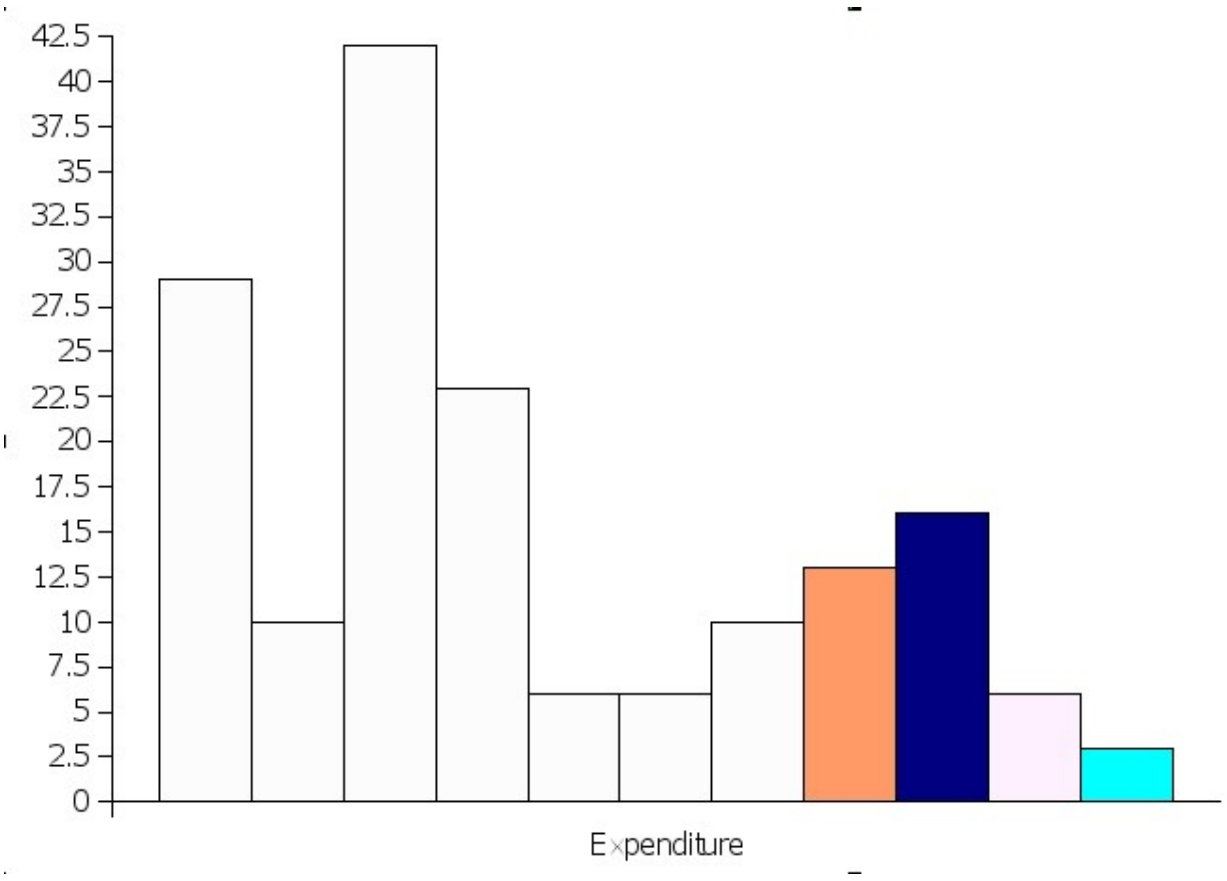
Longest life: 1080 (3 years)

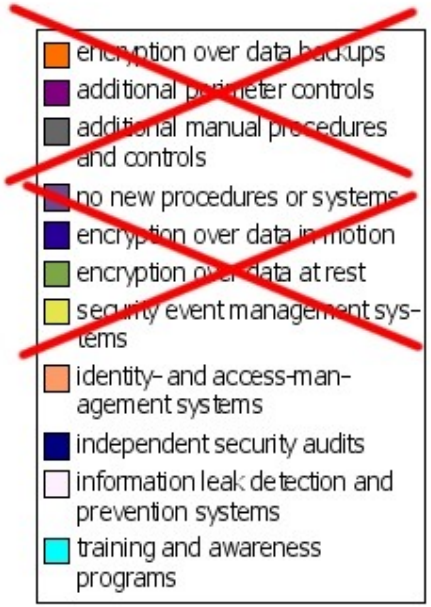
What does 0day mean to you?

- You care when you're hacked, possibly only because
  - your customers care
  - you have to report it
- Attacks cost you money
  - USD $182 per compromised record[1]
  - 27,500 average number of records
  - Average computer security incident response costs $5 million
- You want to detect an attack, and 0days affect your ability to do that

[1]Ponemon Institute, Cost of Data Breach Study, 2006

After Incident: Where the Money Goes





Most of these actions will do nothing to prevent an 0day based incident happening again!

Source: Ponemon Institute, Cost of Data Breach Study, 2006

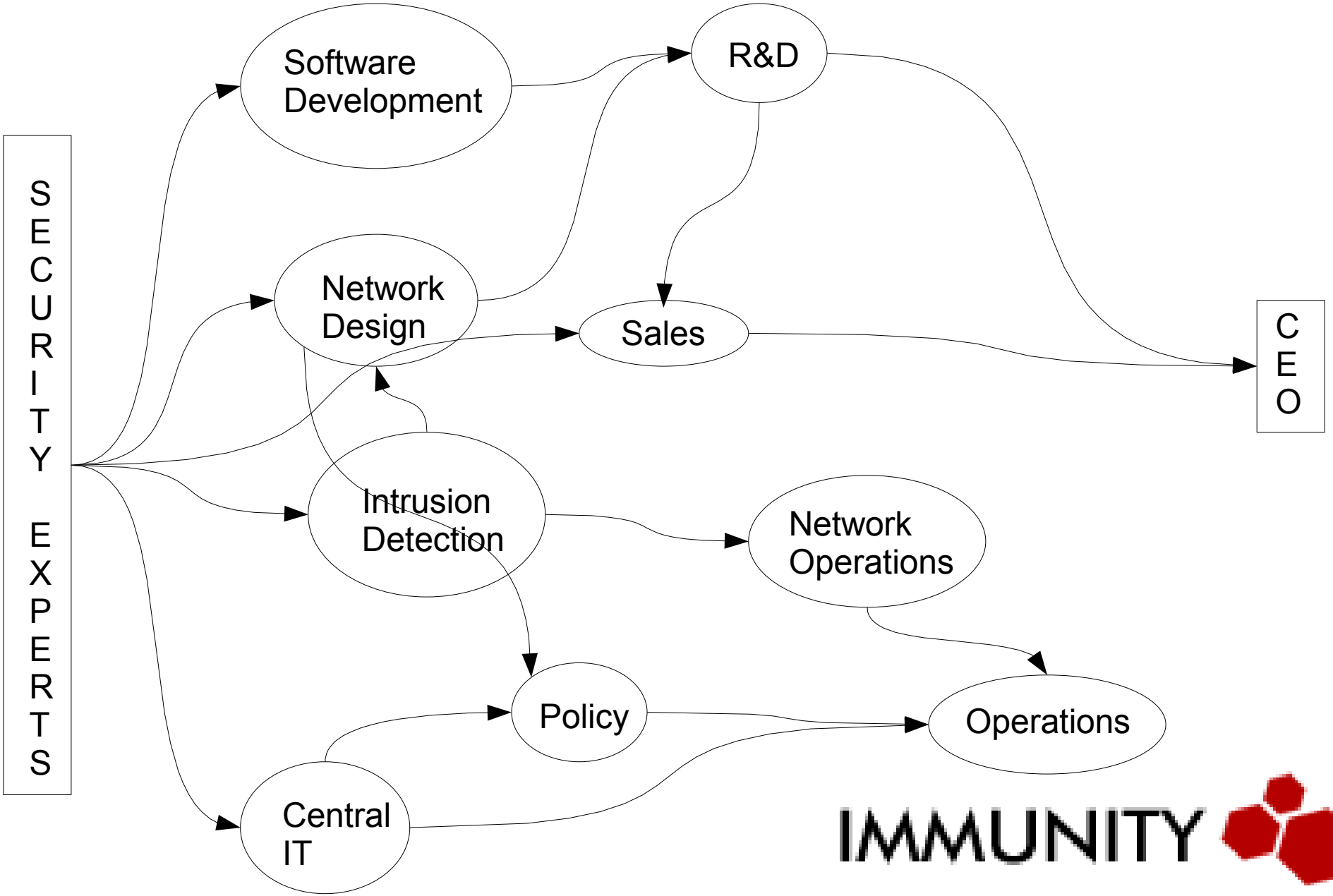
IMMUNITY

Reorganize around the World of 0day

The team, technology, and your business.

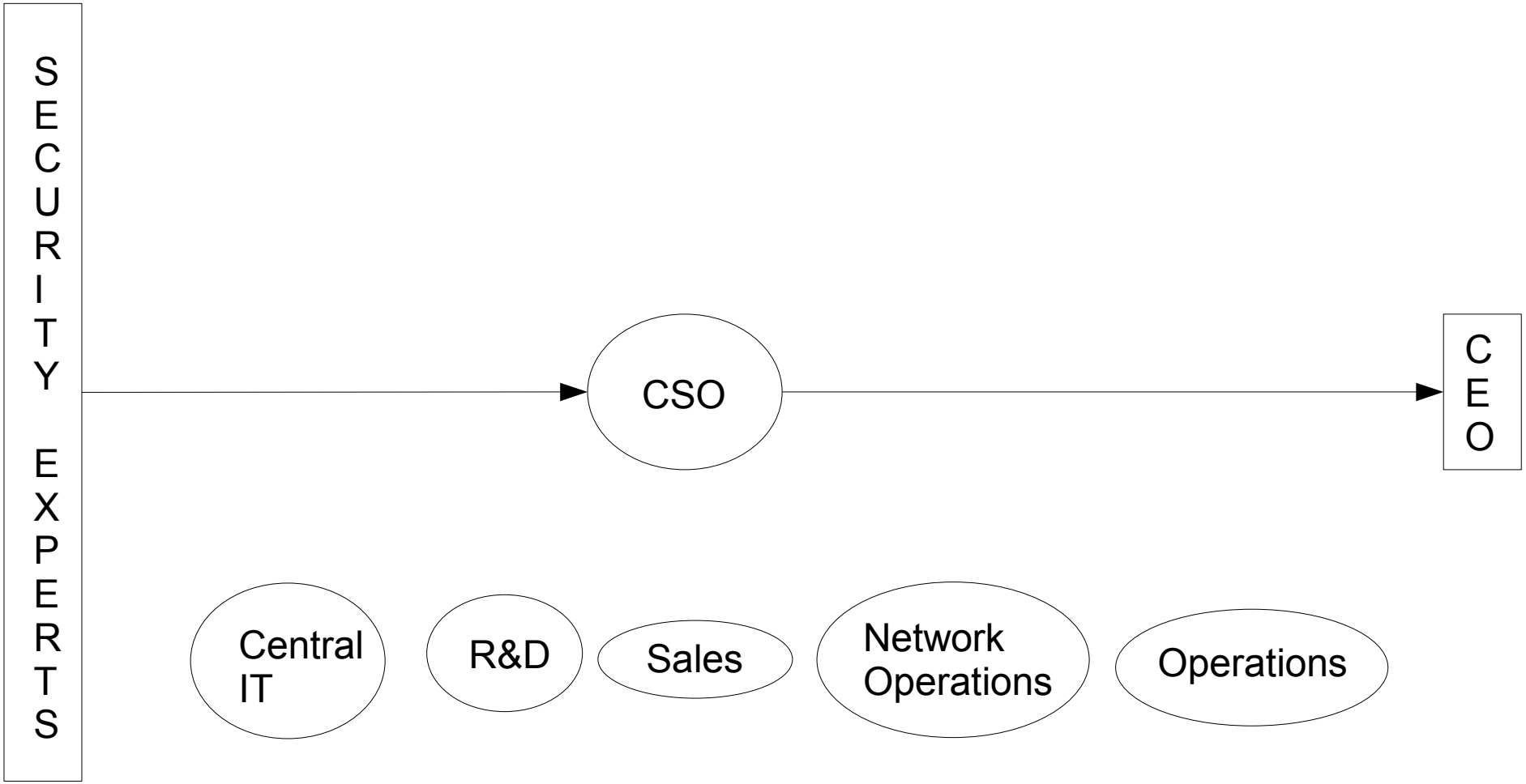
- Build a knowledgeable team, prepare for incident response.
- Less reliance on signature-based IDS/IPS, seek out anomaly detection.
- Executive support and funding are the essential first step.

Reorganize the Business: Before



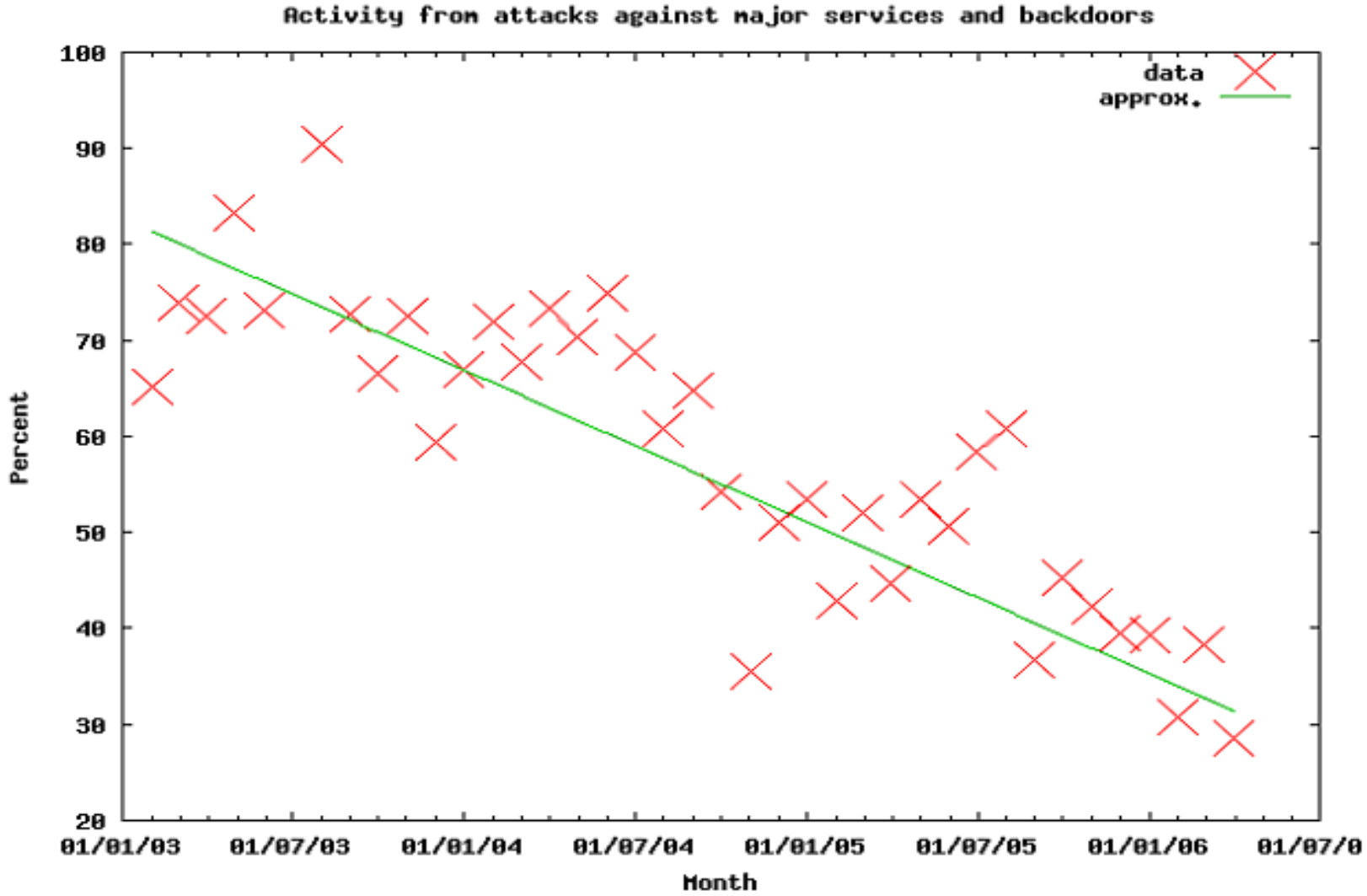
IMMUNITY

Reorganize the Business: After



IMMUNITY

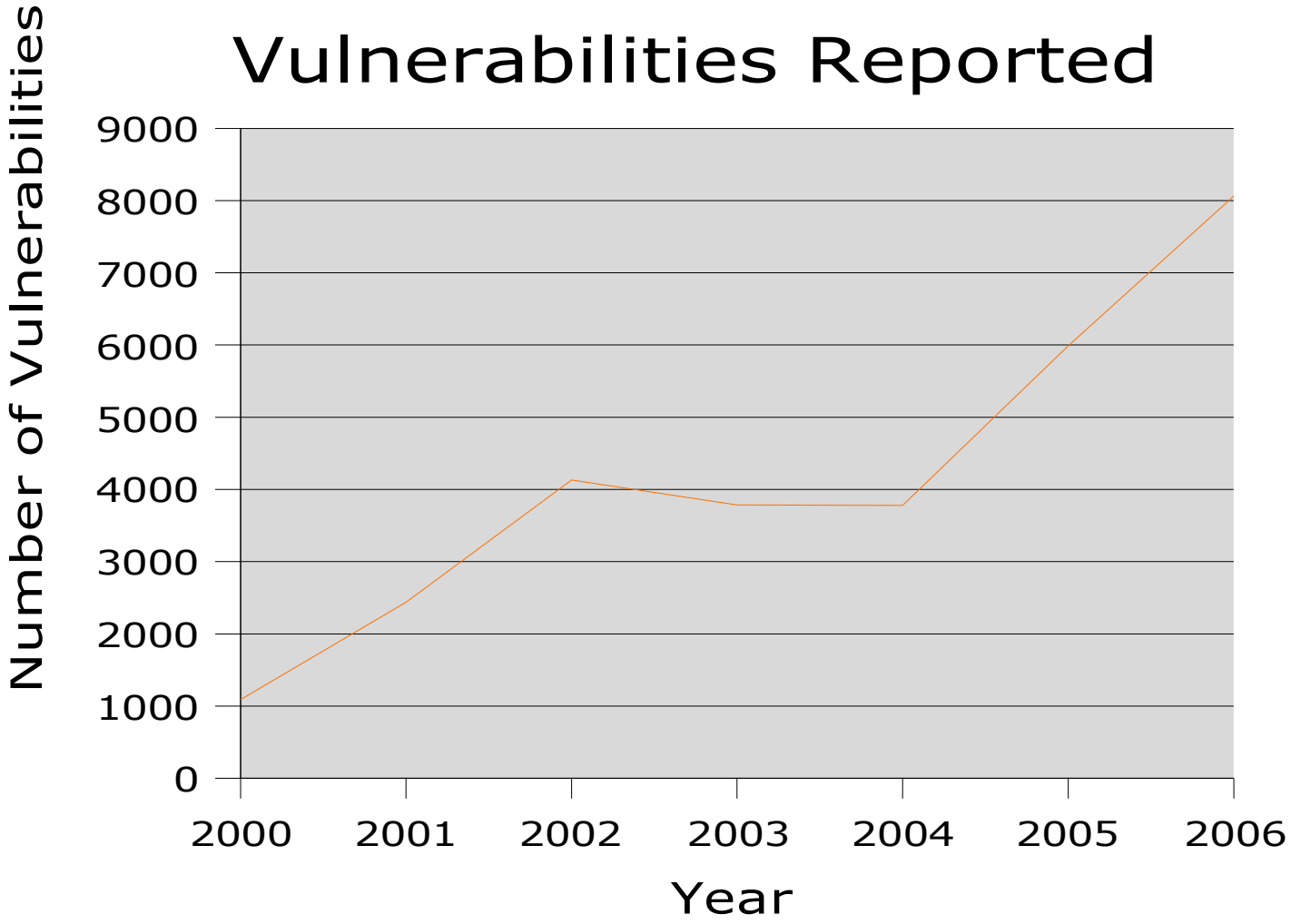
Old school metrics no longer relevant



Source: SANS Internet Storm Center

IMMUNITY

More Irrelevant Metrics



Source: CERT/CC Statistics 1988-2006

IMMUNITY

Making Metrics Work

How many attacks go undetected?

How do you value damage that you don't know about?

New opportunities to measure reality, as the 0day has “IPO”d....

An Intrusion is an Anomaly

IMMUNITY

$1244 bucks says your IDS is completely ineffective

- Sig-based systems do not work
- Where are the anomaly based systems?
  - a proper anomaly based system means a one-time purchase
  - subscription models mean revenue
- Signatures attach all-knowing labels to things (makes pretty “informed” reports for unknowledgeable management)
- An exploit is not a fingerprint

Anomaly vs Signature-based: knowing the difference

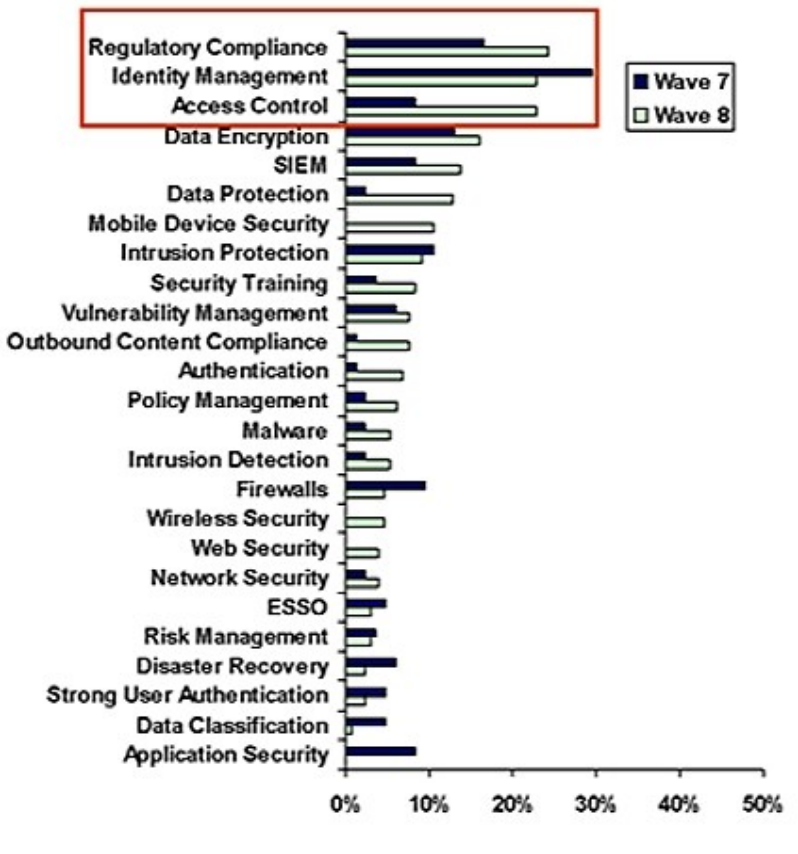
- A signature is a rule, be that a protocol parsing rule, a regular expression, a heuristic.
- If you have to update once a month, you're updating a signature database.
  - lower maintenance costs
- An anomaly-based system shouldn't need to call out or need holes in the firewall
- Anomaly vendor will be able to talk about the system's learning process

Make Yourself Unhackable (or at least know who did it)

- ASSESS YOUR PRODUCTS
  - Always assume the technology has 0day, try to prove yourself wrong
  - Demand results of an independent security analysis or do it yourself (vendor products)
  - If it falls quickly, it's got serious security problems and they are going to affect you
- ASSESS YOUR EXPOSURE
  - Understand via pen testing, in house or external services

IMMUNITY

Compliance & Motives



source: TheInfoPro Information Security Study Wave 8 (7/18/2006)

- US companies spending most on compliance (PCI/SOX/GLBA/HIPAA/etc)
- Pressures on trading systems:
  - need to distinguish between a bad trade and a hacked trade
  - auditing, record-keeping requirements may force clear-text
- Compliance does not address 0day

IMMUNITY

The Role of Scanners and Penetration Testing

- Scanning for known vulnerabilities is just a line item as part of a proper penetration test.
- A professional pen test will include 0day research
- Full and accurate staging systems are essential -> you can't be making accidental trades because the pen testers are forced to assess a production machine!

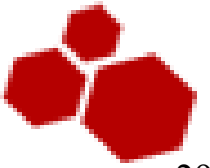
Quality penetration testing

Ask your pen testers what they do about 0day & exploitation

- How can a pen tester know the “severity level” of a vulnerability if they did not exploit it?
- 3 grades of pen testers:
  - top tier: can find 0day and/or can write exploits
  - middle tier: run products written by people who can find 0day/write exploits
  - bottom tier: run vulnerability assessment scanners

If you know enough to hire a low grade pen tester, you know enough to buy the same tool and run it yourself!

IMMUNITY



Make sure its legit: 0day and the Law

1. Keep the senior execs informed and on your side.
2. Get corporate legal team's attention by drawing attention to potential license violation (eg. reverse engineering).
3. Motivate legal to draft wording into your vendor Master Agreements that allows unrestricted security testing.

People are better than technology

- Do hire hackers
- Information security people present special problems
- Exploit developers are different from the people who run IDS's
- How does this affect your training plan?
- Team relationship with other departments
- Finding solutions may be a different problem to identifying problems
- Get ready for incident response
- Intellectual Property management

Hackers on the Trading Floor

- Critical, complex, untouched trading and financial systems are attraction enough
- Understand the politics (eg vuln disclosure) before you hire
- Fuel the ego (require 0day discovery)
- Open the ports (they need IRC like a fish needs water)
- Encourage normal working hours by demonstrating all the great reasons to knock off work at 6pm
- Never ever require any kind of dress code
- Create a safe environment (hackers tend to be cautious by nature)

IMMUNITY

Incident Response

- More than network reconfiguration
- Think memory dump analysis
- Takes a hacker to know a hacker
- The tools are more expensive but easier to use than you think (you need the calibre of person who can learn to use a tool on the fly)
- Communicate:
  - Give them a cell phone and encourage them to make it part of their lives, find out where they hang online

More Ways to Make Yourself Unhackable

Engage in community and do what the hackers do.

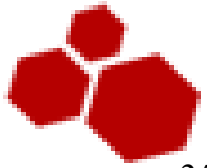
Trading Systems achievements so far:

- 2 factor authentication (increases the attacker's need for a residential solution trojans/keyloggers/etc)
- Virtualization

IMMUNITY

Immunity's Role in the New World of 0day

- Teaching how to find 0day
- 0day/exploit purchasing program
  - Immunity values lifespan and does not disclose
  - first to start time-based compensation model
- Attack only
- Information management and propaganda resistance
- CANVAS is a platform
- Making exploit developers lives easier
- Teaching what to do with an 0day when you've found it

IMMUNITY 

What you need to do, now.

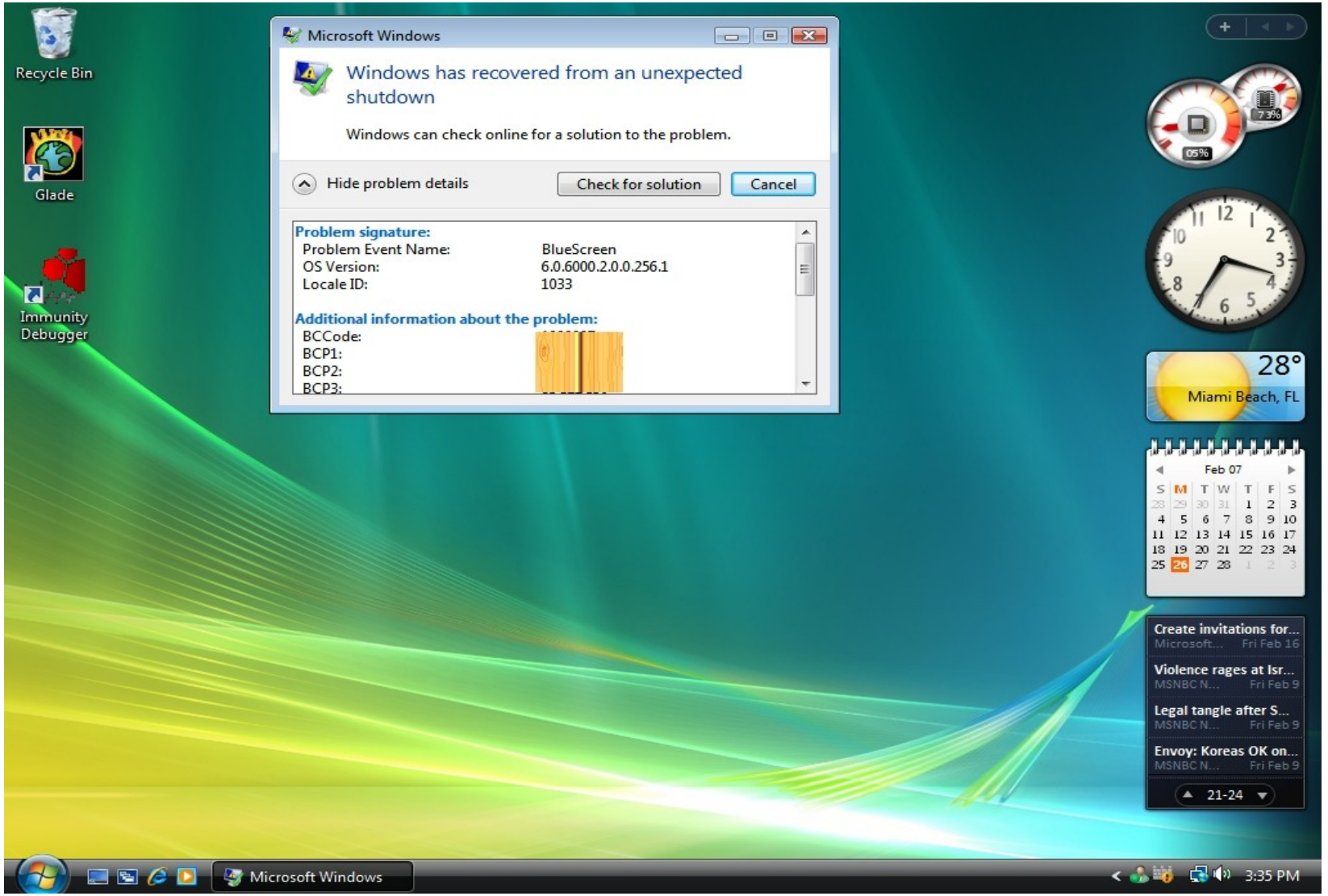
- How many applications have you got facing the Internet?
- Who last assessed them and when?
  - If they didn't find an 0day, the assessment wasn't good enough
- Get your applications assessed and your developers security-aware.

“There is a crack in
everything
That's how the light gets in.”
- Leonard Cohen

The Future

- Worms
  - No-one is prepared for worms targeting custom infrastructure, such as proprietary trading systems
- Automated Exploit Development
  - Our time to exploit is shorter than your ability to patch
- Vulnerability Marketplace
  - more transparency and increased ability for us to understand our real exposure

Thank You



IMMUNITY