

# Information Security Is a Business Continuity Issue: Are You Ready?

Dr. Nader Mehravari

Cyber Risk and Resilience Management Team  
CERT Division  
Software Engineering Institute  
Carnegie Mellon University  
nmehravari@sei.cmu.edu  
<http://www.cert.org/resilience/>

# Notices

---

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0002411

# Four Key Functions of a Modern CISO

Focus of  
Today's Discussion

**Protect / Shield**



**Monitor / Hunt**



**Recover / Sustain**



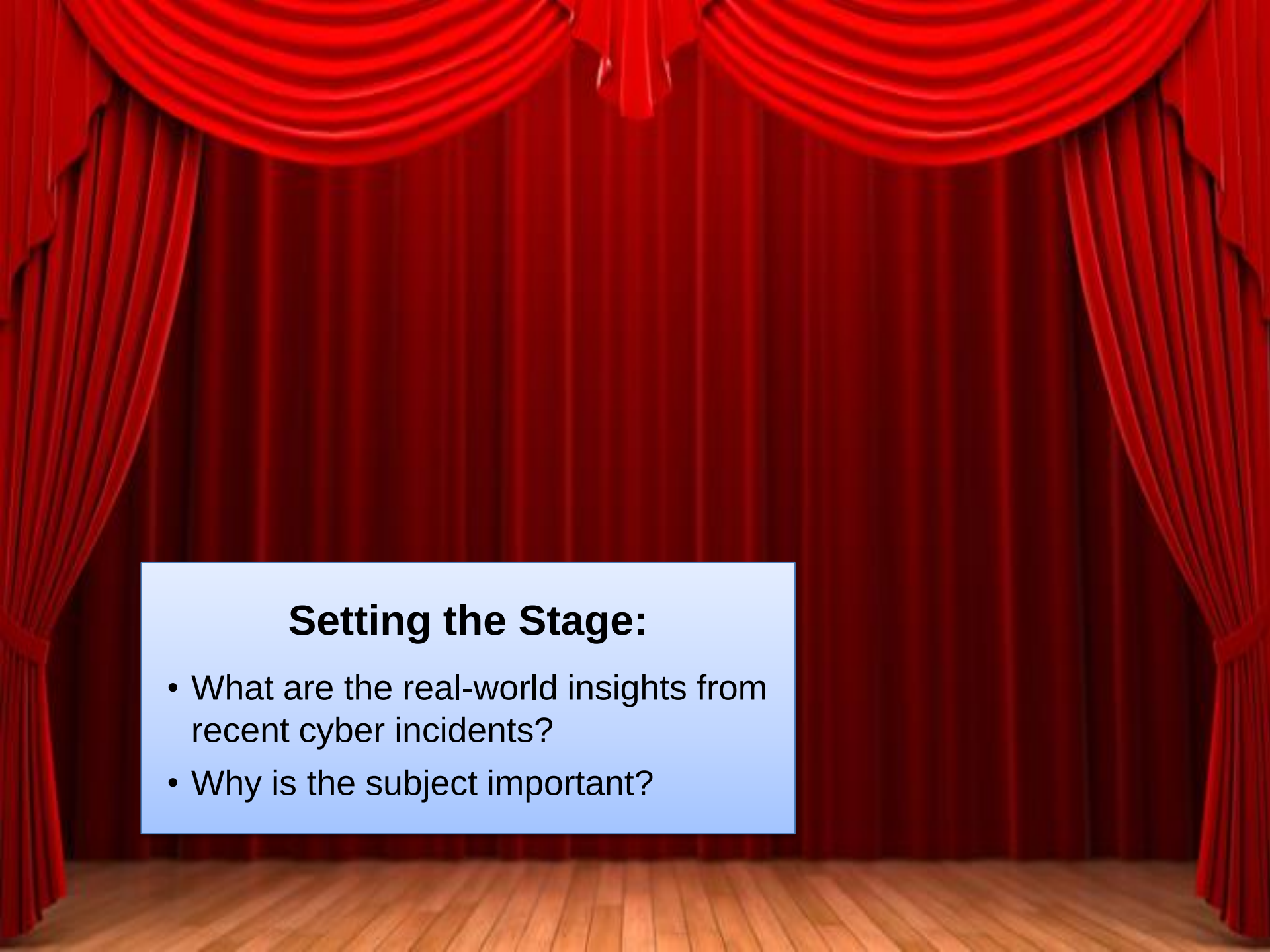
**Manage / Govern**



# Key Issues

---

- What are the real-world insights from recent cyber incidents?
- How does preparedness planning for cyber incidents differ from traditional BCM planning?
- How can organizations align BCM with their cybersecurity efforts?

The background of the slide is a photograph of a stage. It features heavy red curtains with a scalloped top edge, hanging from a central point. The curtains are pulled back slightly on the sides, revealing a light-colored wooden floor with a vertical grain pattern. The lighting is soft, creating a professional and formal atmosphere.

## **Setting the Stage:**

- What are the real-world insights from recent cyber incidents?
- Why is the subject important?

# Cyber Intrusions are a Fact of Life



U B E R



JPMORGAN CHASE & CO.



Forbes



ebay



Anthem



# Prevention Activities Fall Short

- Is necessary
- Is not Sufficient
- Fails too frequently

**Protect / Shield**



**Monitor / Hunt**



**Recover / Sustain**



**Manage / Govern**



*...there are only two types of companies:  
those that have been hacked and those that  
will be...*

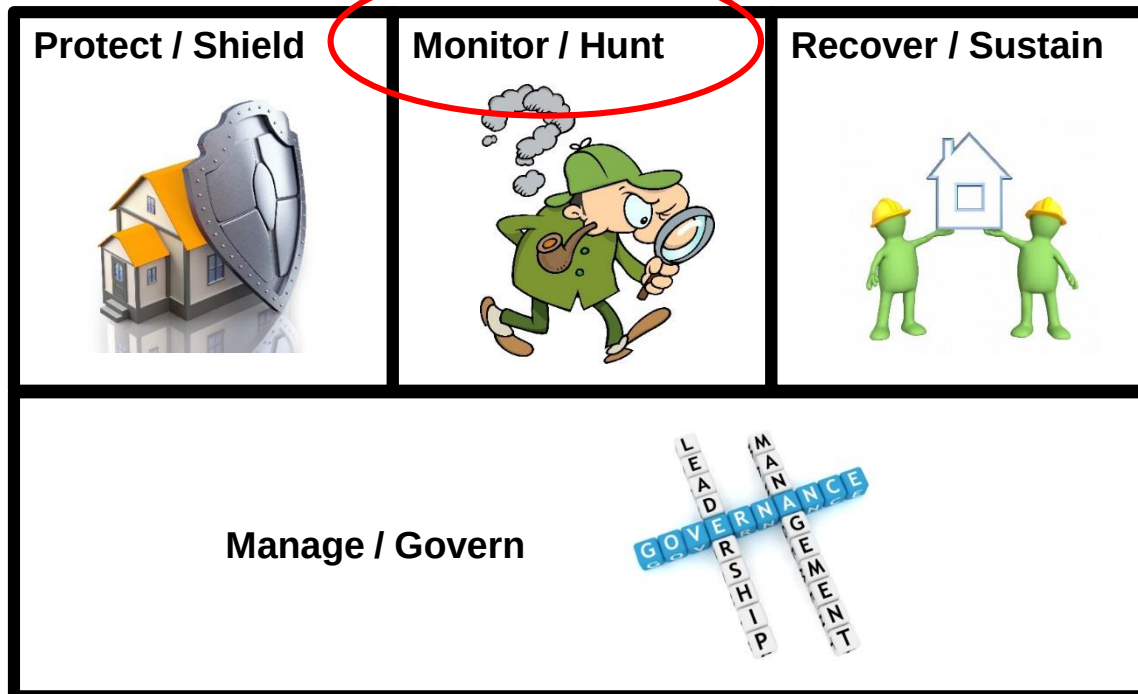
*...and even they are converging into  
one category: companies that have  
been hacked and will be hacked  
again...*

*Robert S. Mueller, III  
Former Director of FBI  
March 1, 2012*



# Prevention Activities Fall Short

- Is necessary
- Is not Sufficient
- Not immediate
- Takes too long



# Targeted Attacks are Hard to Detect

- How are compromises detected?
- How long before the compromises are detected?

69%

of victims were notified  
by an external entity

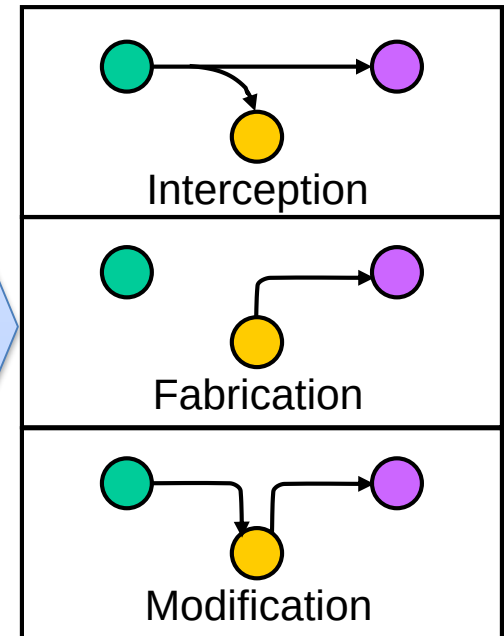
205

median number of days  
before detection

SOURCE: Mandiant® “M-Trends® 2015: A View from the Front Lines” Report

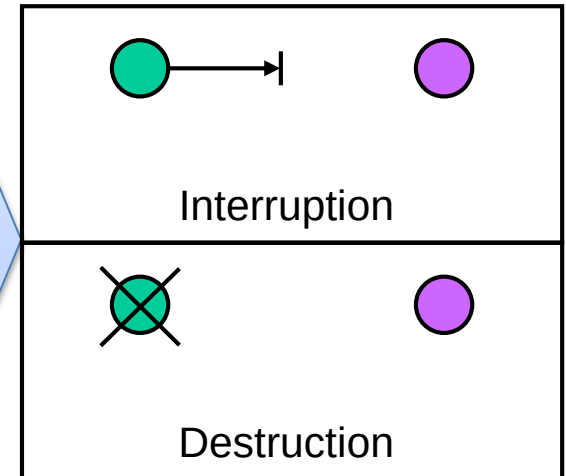
# Most Frequent Cyber Attacks Fallout

- Disclosure of operationally sensitive information
- Disclosure of privately identifiable information
- Theft of intellectual property
- Theft of user access credentials
- Loss of credit card information
- Disclosure of classified information
- Revealing of company proprietary information
- Exposure of corporate email messages
- Identifying oppositions and enemies
- Leak of trade secrets
- Nuisance
- Reputation damage
- Hacktivism - Delivering political or social message
- Blackmailing



# However, adversaries are interested in more...

- Deleting and destroying data
- Causing operational havoc
- Physical harm to people
- Physical damage to infrastructure
- Destruction of physical goods
- Damaging critical infrastructure
- Affecting delivery of products and services
- Shutting down day-to-day business operations



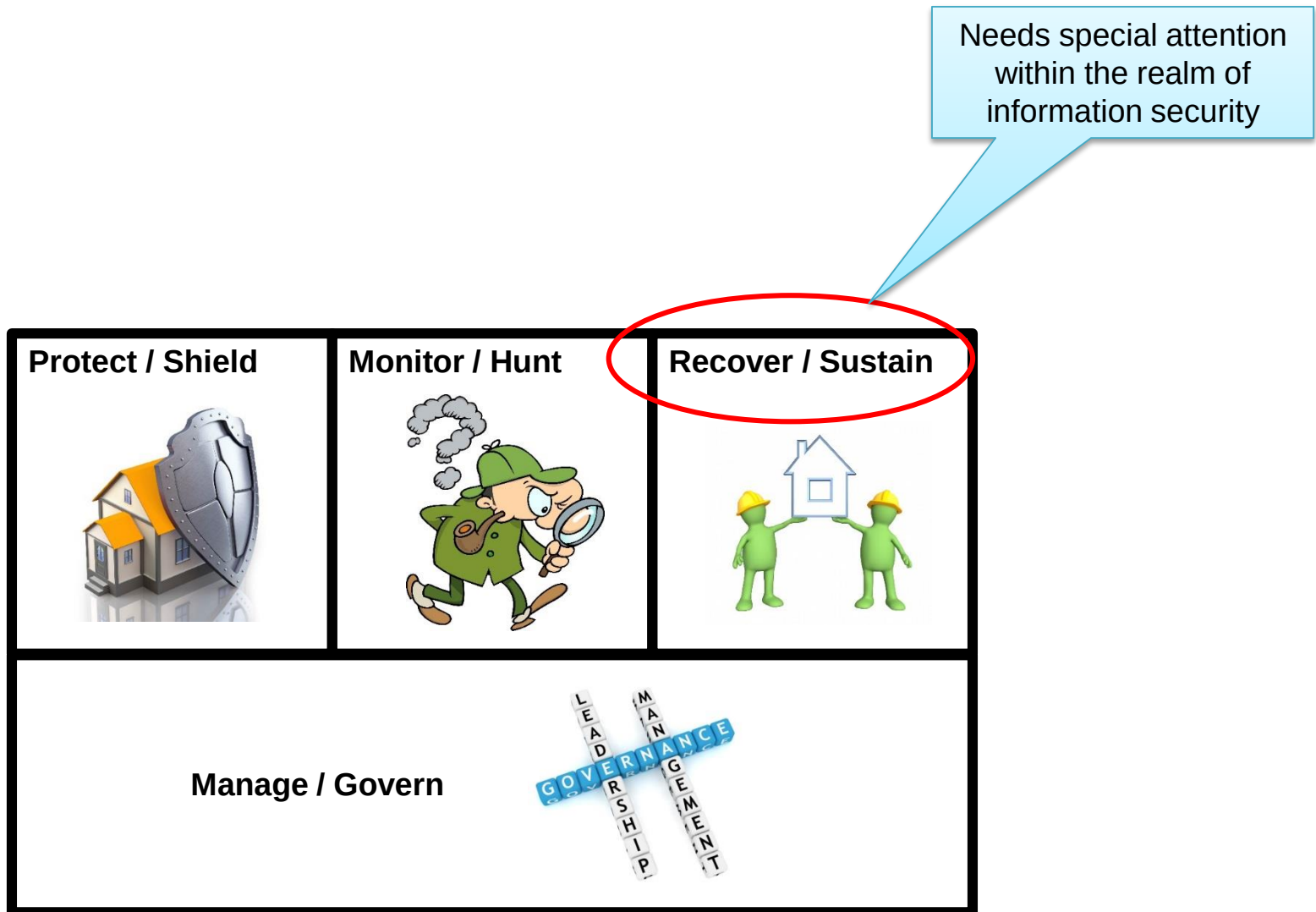
# Example: Sony Pictures Cyber Incident

---

- Reputation
- Revenue Loss
- Data Exfiltration
  - Over 100 terabytes
- **Business Operations**
  - Damaged information technology infrastructure
  - Hackers implanted and executed malware that destroyed data
  - Malware with capability to overwrite master boot records and data files
- Legal
  - Employees have filed four lawsuits against the company for not protecting their data
- Breach Expenses
  - In its first quarter financials for 2015, Sony Pictures set aside \$15 million to deal with ongoing damages from the hack.



# and therefore...





## **Guidnace:**

- How does preparedness planning for cyber incidents differ from traditional BCM planning?
- How can organizations align BCM with their cybersecurity efforts?

# Considerations for...

Developing

- Business Continuity
- IT Disaster Recovery
- Incident Response
- Crisis Management
- Continuity of Operations
- Emergency Management
- Crisis Communications
- Workforce Continuity
- Etc...

plans for execution in cyber-affected environments

Executing

plans in cyber-affected environments



# Consider This Scenario

---

- Adversary's long-term and established presence in your environment has been confirmed (e.g., through investigative and forensic activities).
- Adversary has been observing and learning your environment for some extended time.
- Adversary has proliferated customized malware on strategic elements of your IT and operational technology (OT) infrastructure.
- Adversary has exfiltrated confidential information.
- Adversary has just made operationally disruptive moves, for example
  - Physical and logical damage to IT infrastructure
  - Physical and logical damage to OT infrastructure
  - Data destruction
- Day-to-day business operations have negatively been affected

*i.e., it is time to execute one or more of your preparedness plans*

# Things to Consider (i.e., Dilemmas)

---

Do you try to get the adversary out of your environment before starting recovery and restoration activities?

Yes?

- Have you finished investigative and forensic activities before disturbing the adversary?

# Things to Consider (i.e., Dilemmas)

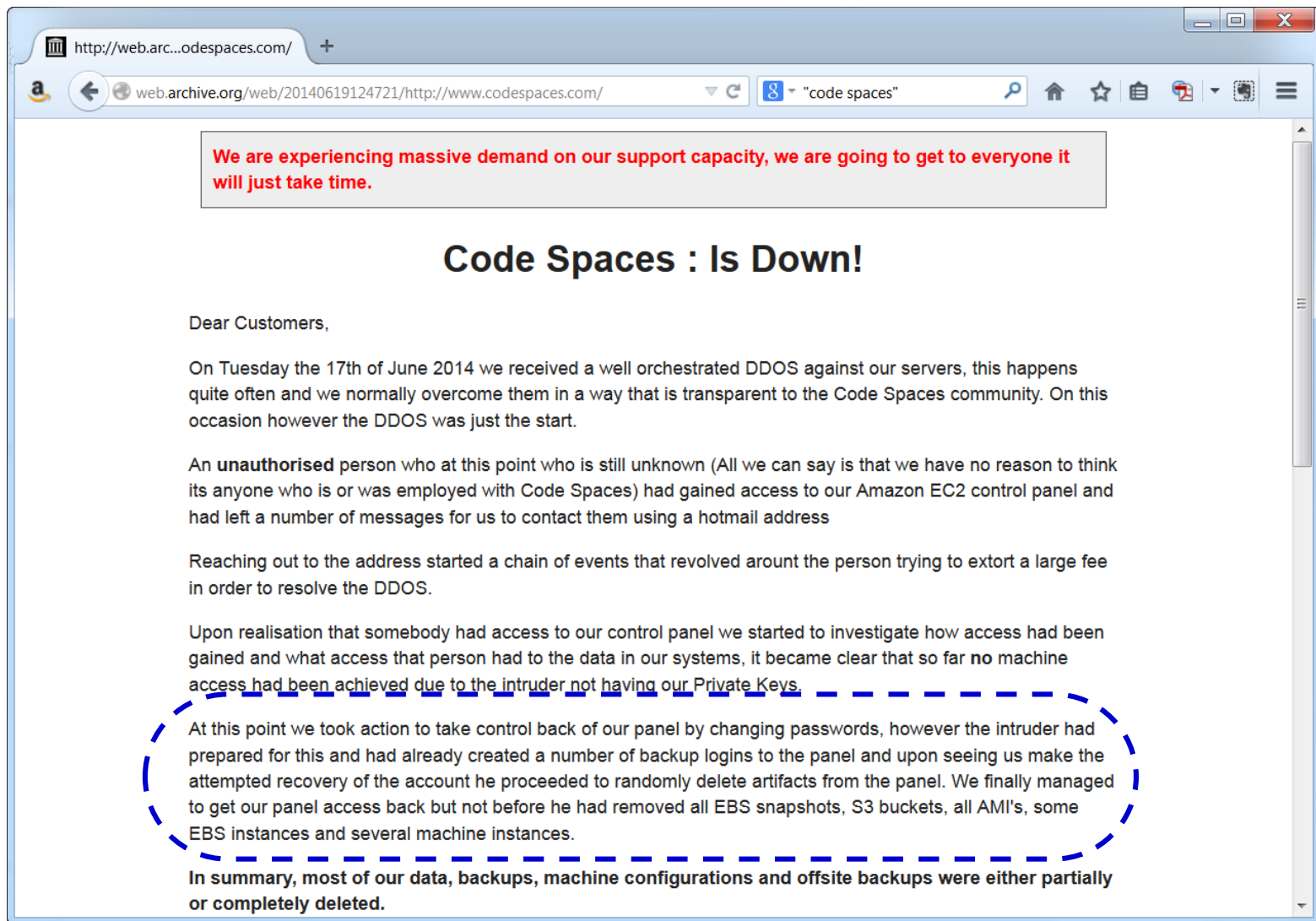
---

Do you try to get the adversary out of your environment before starting recovery and restoration activities?

Yes?

- Is there a chance that the adversary may try to do major damage if it notices that you are trying to kick it out?

# Example: Cyber Attack on Code Spaces



**We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.**

## Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far **no machine access had been achieved due to the intruder not having our Private Keys.**

At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel. We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances.

In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted.

# Things to Consider (i.e., Dilemmas)

---

Do you try to get the adversary out of your environment before starting recovery and restoration activities?

Yes?

➤ How long will it take you to get the adversary out?

*(What did you say was your RTO?)*

# Things to Consider (i.e., Dilemmas)

---

Do you try to get the adversary out of your environment before starting recovery and restoration activities?

Yes?

- How will you be sure that the adversary is no longer around?

# Things to Consider (i.e., Dilemmas)

---

Do you try to get the adversary out of your environment before starting recovery and restoration activities?

**No?**

- Is your enterprise systems (e.g., email, Internet access, file shares, printers, PBX, VoIP) available?
  - YES:
    - Then the adversary is most probably monitoring (listening) to every move you make.
    - How will you keep your execution plan a secret?
  - NO:
    - Do you have alternative system (not on your infrastructure) that you can use to manage the incident?

# Things to Consider (i.e., Dilemmas)

---

Do you try to get the adversary out of your environment before starting recovery and restoration activities?

No?

- While rebuilding damaged/destroyed/corrupted systems, how would you ensure that the adversary won't get into these newly built infrastructure while building them on your currently (infected) environment?



# In Closing



# Modern Cyber Attacks Can Disrupt...



People Assets



Technology Assets

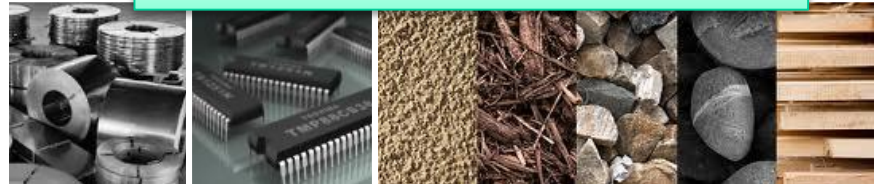
Information Assets



Facilities Assets



Supply Chain / Raw Material Assets



... not just information assets

# Therefore,

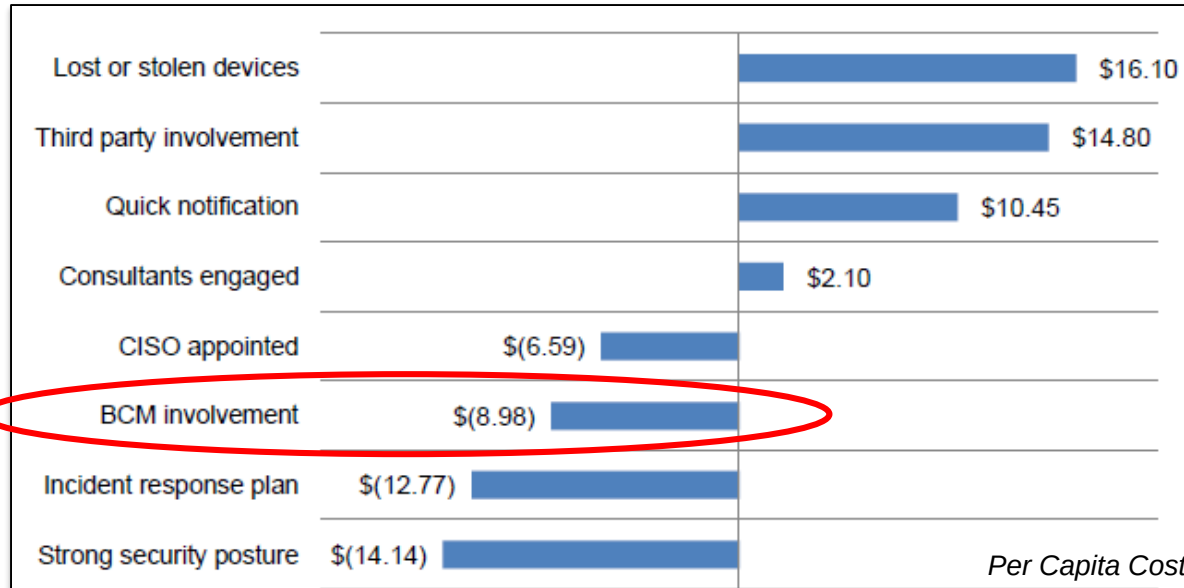
---

## All preparedness planning activities...

- IT Disaster Recovery
- Business Continuity
- Continuity of Operations
- Emergency Management
- Incident Response
- Crisis Communications
- Workforce Continuity
- Etc...

... must explicitly incorporate matters related to cybersecurity risk, cyber attacks, and cyber-enhanced incidents into their planning, testing, and execution processes.

# Factors Affecting Cost of Data Breach



**Business continuity management reduced the cost of a breach.** For the first time, the research reveals that having business continuity management involved in the remediation of the breach can reduce the cost by an average of \$8.98 per compromised record.

SOURCE: Ponemon 2014 Cost of Data Breach Study





**Thank you for your attention.**