

Risk Management through Security Planning

Boston University Security Camp, August 21, 2014

PATTY PATRIA
CIO
BECKER COLLEGE

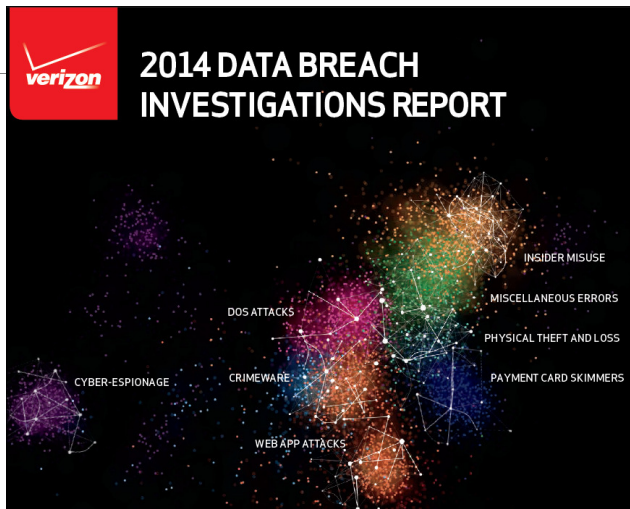


DAVID SHERRY
CISO
BROWN UNIVERSITY

The state of security 2014

Let's set some context.....

2014 Threat Landscape



Verizon 2014 Breach Report

- 63,000+ reported incidents
- 1,367 confirmed breaches
- 110 million consumers in the Target breach alone

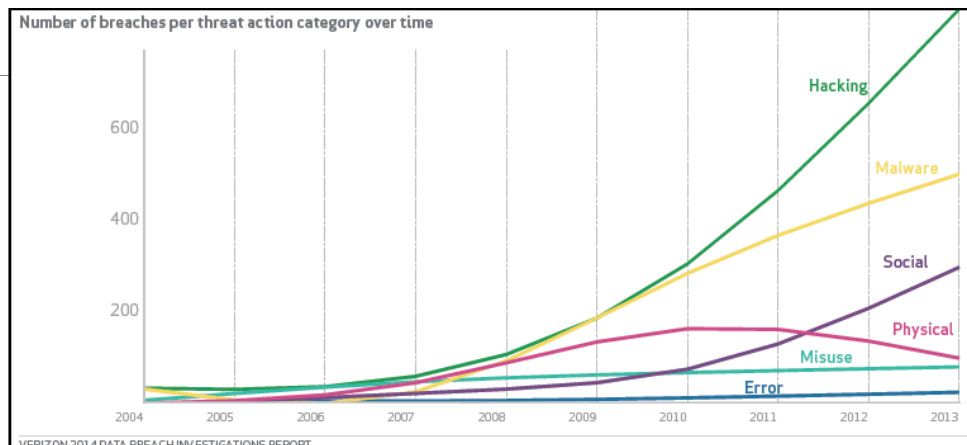


Ponemon Data Breach Costs

- Average cost of breach is \$5.4 million
- More than \$136 per compromised record
- Cost of detection, response, notification and lost business

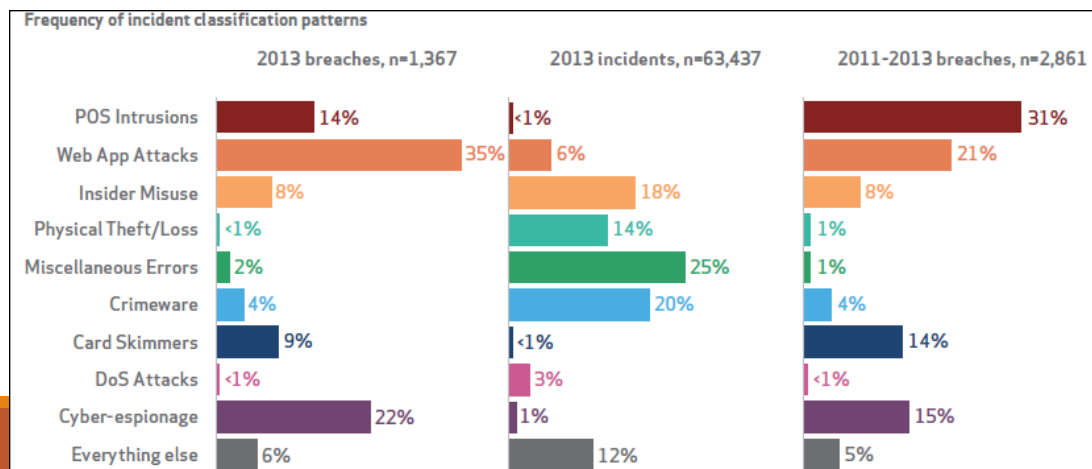
Source: www.ponemon.org and www.verizonbusiness.com

2014 Threat Landscape

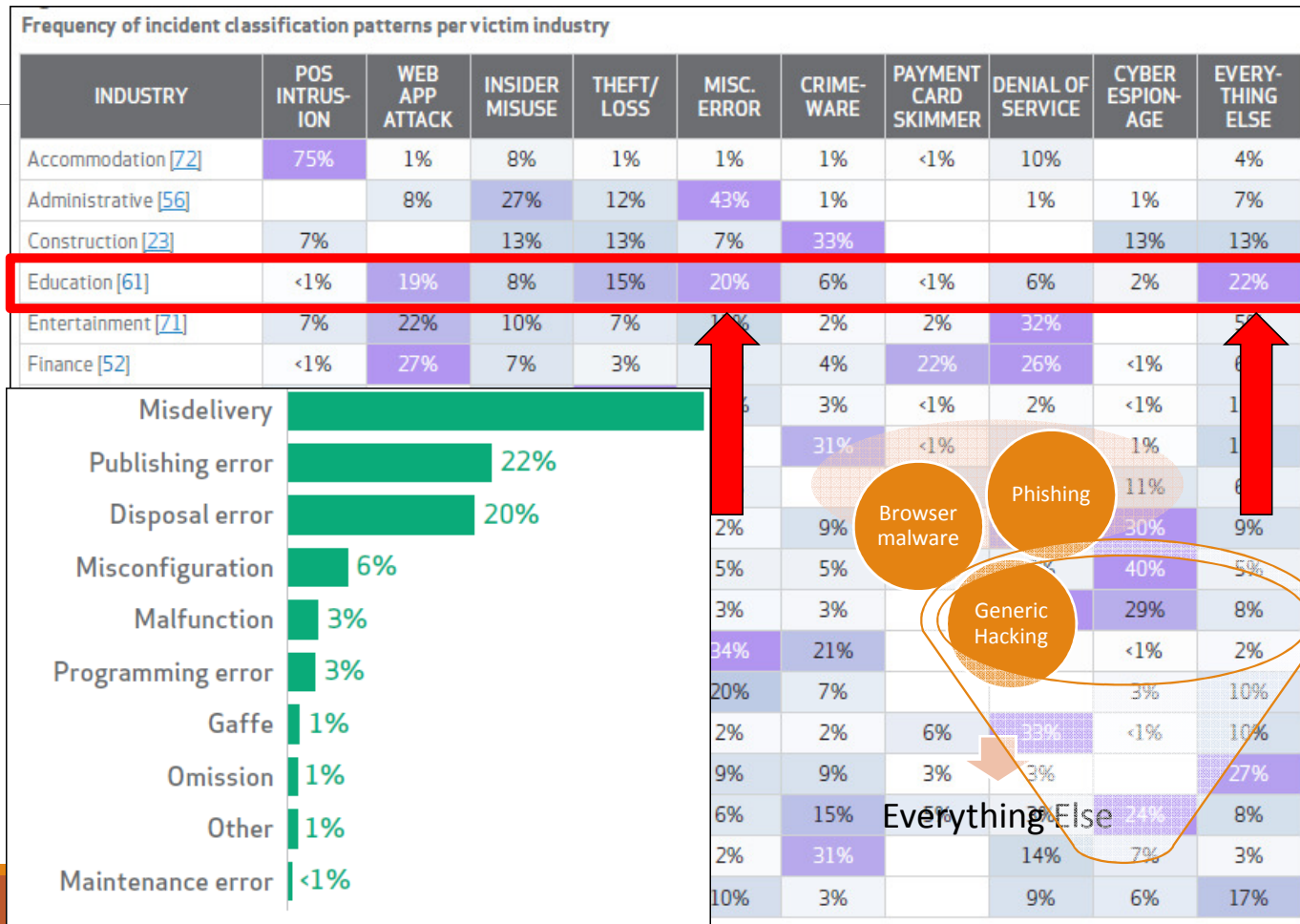


- **Hacking, Malware and Social Attacks are on the rise**

- **POS and web application attacks top threats**



2014 Threat Landscape



The attacks are continuous (map.ipviking.com)



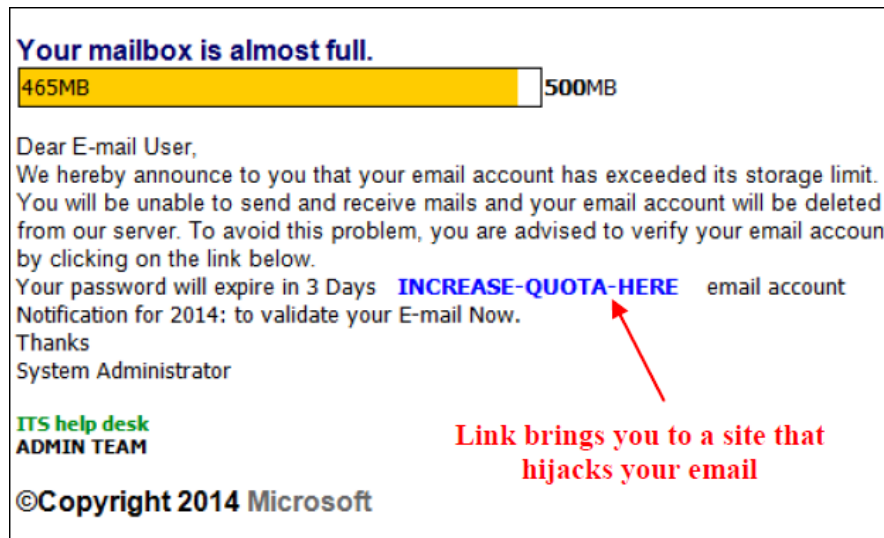
Recent Threats Affecting Becker and Brown

We have a feeling that you've seen some of these as well.....

Recent Threats Affecting Becker

Repeated responses to email Phishing several times this year.

- Employees respond to illegitimate email messages.
- Hijackers take over your email, send spam and Becker gets blacklisted, causing email to external recipients to be blocked.



Recent Threats Affecting Becker

Ransom Ware incident on L Drive and Vet network share.

- Employee clicked a link in personal email (from Becker computer) and it encrypted all files on their personal computer, Vet share and L drive.
- Files were encrypted and could not be opened. Encryption process ran for 36 hours before detected.
- We had to restore from backups 2 days prior to get all files back.



Recent Threats Affecting Brown

Getting attention via “salary update” phishing scam

- Widespread attack on 7/30/14
- Appeared to have come from HR
- Had the Brown logo (though skewed)
- Had “sincerity”



BROWN

----- Forwarded message -----

From: **BU-HR** <employeebenefits@brown.edu>

Date: Fri, Jul 25, 2014 at 4:21 PM

Subject: Important Salary Update

To: david_sherry@brown.edu

Hello,

The University is having a salary increment program again this year with an average of 2.5%

The Human Resources department evaluated you for a raise on your next paycheck.


Click below to confirm and access your salary revision documents:

[Click Here](#) to access the documents

Sincerely,
Human Resources
Brown University

Recent Threats Affecting Brown

← → ↻ http://bunnylove.ru/www.brown.edu/Login.htm

 BROWN UNIVERSITY

Authentication Required


Enter your Brown credentials

Username: *

Password: *


[Continue](#) [Forgot your password?](#)

You have asked to log in to:



BROWN

[Brown Home](#) | [Help](#) | **New Users:** [Activate your account now](#)

 Shibboleth. Need to know more? Learn more about [Shibboleth at Brown](#).

BROWN UNIVERSITY
Providence, Rhode Island 02912, USA
Phone: 401-863-1000
[Maps & Directions](#) / [Contact Us](#)
© 2013 Brown University

Recent Threats Affecting Brown

This one really hit home!

- A very common phishing scam
- With an uncommon subject line
- Proof that the scammers were in another box when we contacted them

From: **Brown University Mail** <student@brown.edu>
Date: Wed, Aug 6, 2014 at 4:22 PM
Subject: Message from Brown Information Security: Your email account has been compromised
To: david_sherry@brown.edu


MAINTENANCE CENTER.

Dear Brown User,

Attention you have almost exceeded your account mailbox storage quota.
To update or upgrade this process click the link below. Please [*Click Here*](#)

Webmaster Support


The Bottom Line

- Higher Education is a target
 - It will continue to be a target
 - It doesn't matter what your Carnegie designation is
 - It's all about risk
 - We must be prepared
- 

Key take-away

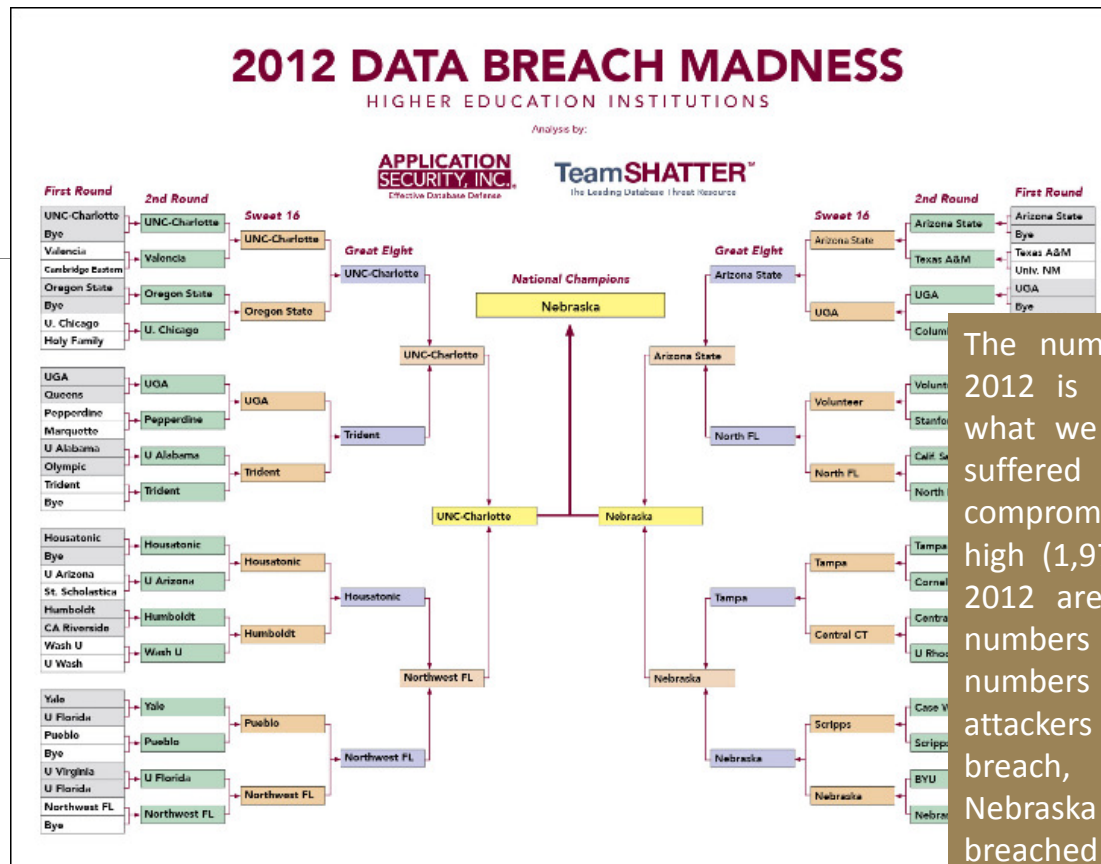
You can reduce risk through security planning

Security planning to address risk

- Ensure executive level buy-in
 - Form an Information Security Advisory Committee
 - Get plugged in
 - Review and develop policies
 - Strategic use of audits
 - Implement technology
 - Train and educate users
 - Purchasing and contract reviews
 - Insurance and breach retainers
 - Incident response
- 

Ensure Executive-Level Buy-In


- Leverage statistics on cost and impact of security threats and breaches to gain support from your President or Chief Administrative Officer.
- Ensure that they know that you will never be 100% secure
- “When”, not “if”
- Always use the term “incident”, and only use “breach” when speaking of actual events
- Get time in front of the Board/Cabinet/Trustees/etc, and not just for bad news
- Be prompt in informing them of the security posture relative to the breaches and findings of other schools
- Speak in terms of dollars and reputation, and less about fear, uncertainty and doubt



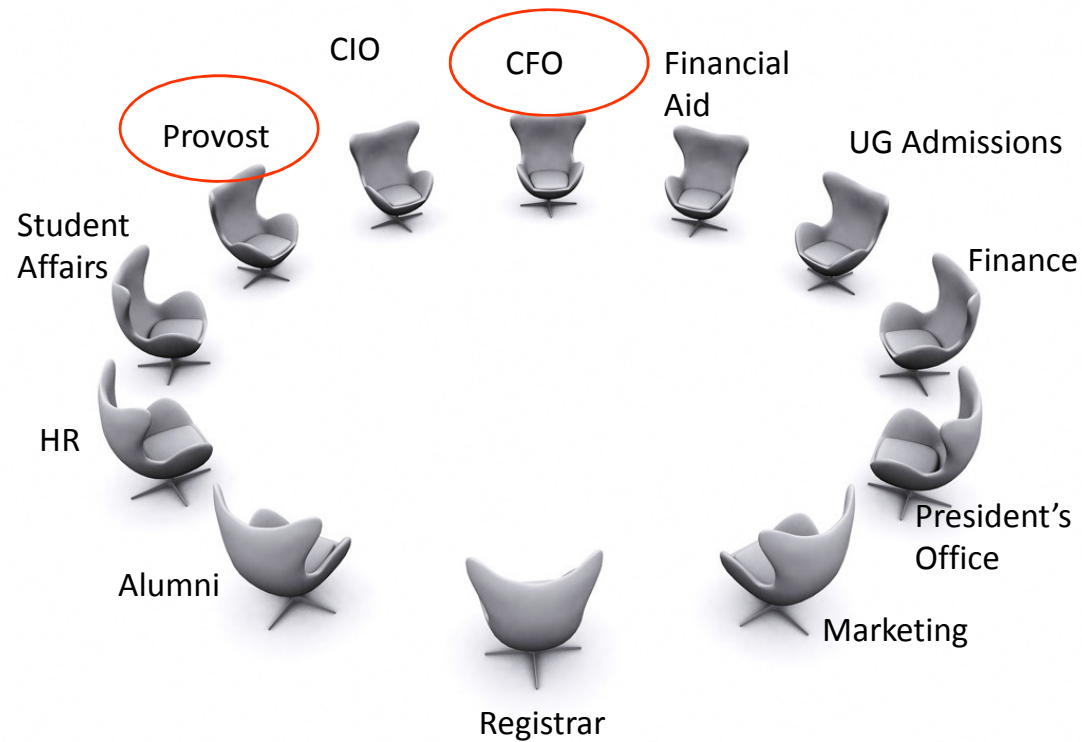
The number of reported breaches in 2012 is relatively low compared with what we have seen in past years (51 suffered breaches), the number of compromised records is at an all-time high (1,977,412). The records stolen in 2012 are more than three times the numbers in 2011 (478,490). These numbers just show how smart the attackers are getting – when there IS a breach, it does quite the damage! Nebraska was the winner for most breached records (650,000 records).

Source: <http://www.teamshatter.com/uncategorized/no-questionable-calls-here-the-march-madness-meets-higher-education-data-breach-brackets-are-back-2/>

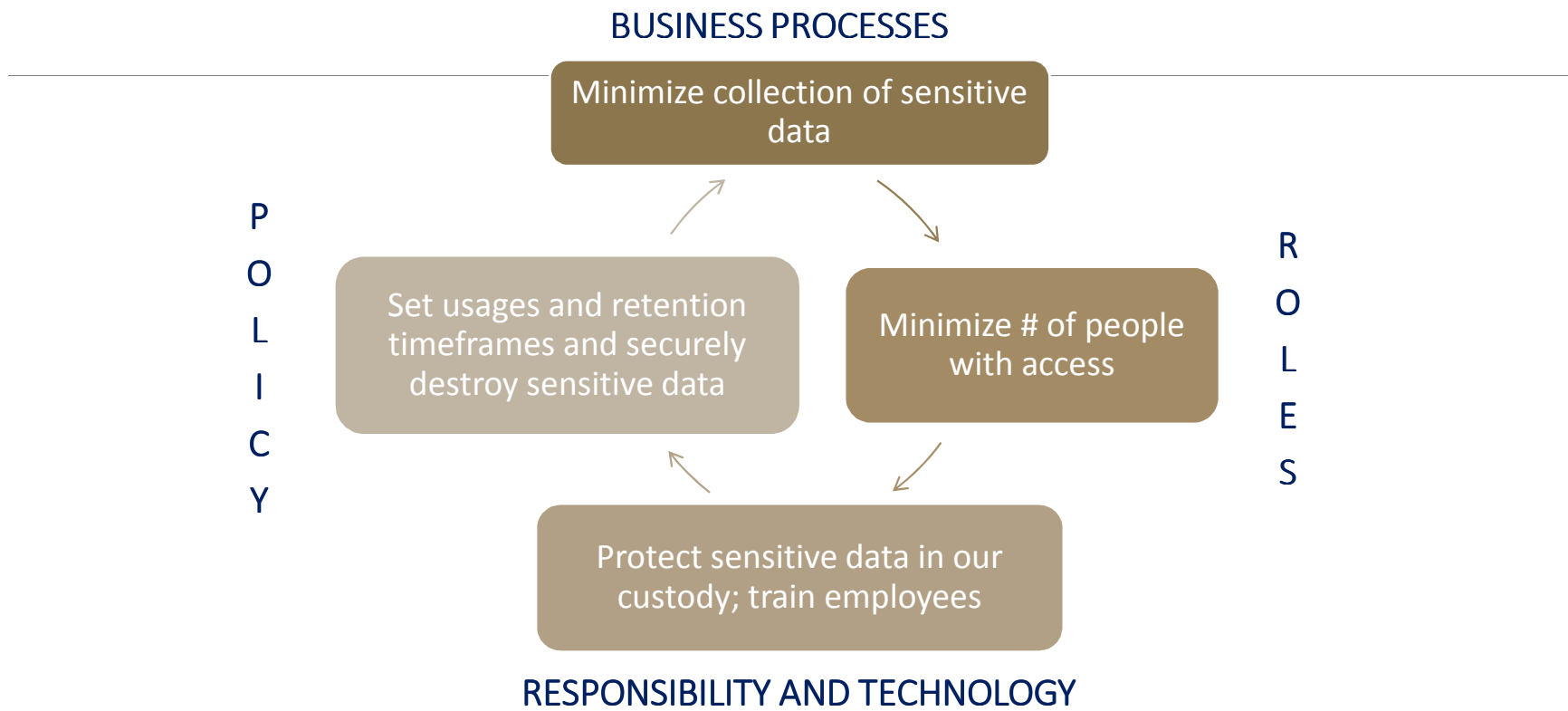
Form an Information Security Advisory Committee

- Ideally have director level (or above) participation from all key departments on campus, especially those the process or store PII.
 - Committee should not be chaired by IT (although IT can run it). Needs to be chaired by Cabinet level folks with influence to address security policy, process and technology.
 - Use the committee to aid in policy review, setting priorities, getting buy-in, and as early adopters
- 

Vet Policy Through a Committee



Enlist Committee's Support in Establishing a Risk Management Framework



Brown's expanded committee and mission

Data, Privacy, Compliance and Records Management Executive Committee (“DPCRM”)


Membership:

SVP of Corporation Affairs and Governance	University Registrar
Vice President of Research	AVP, Research Administration
University Librarian	AVP Financial & Administrative Services
Assistant to the President	Chief Information Security Officer (CHAIR)
Director, Human Resources Services	University Archivist
Chief General Counsel	University Records Manager
Chief University Auditor	Director of International Research Administration
University Controller	Director of Environmental Health and Safety
	Associate Director of Web and Information Services

Get plugged in

- Get a seat on the University Risk Committee (and get a standing agenda item)
- Get a seat on the University Change Control Committee
- Get in the approval line in the IT Project Management process
- Get a seat on the IRB, OSP and HPC committees
- Data use Agreements
- Hospital/University HIPAA Committee
- Make sure your institution knows who your senior security person is!

Review and Develop Policies

- A strong (and up to date!) policy set lowers risk
 - Perform regular gap analysis for emerging areas (times change!)
 - Ensure that all policies are current
 - Maintain a regular schedule of review, and document for auditors
 - Utilize the partnership with Internal Audit to keep current at the landscape of policies
- 

Key Information Security Policies

Confidentiality Agreements & Acceptable Use Policy

Retention and Destruction Policy

Mobile Device Policy

Clean Desk Policy

Digital Millennium Copyright Policy

FERPA & HIPAA Policies

PCI Policy & Red Flags

Gramm-Leach-Bliley Policy

Third Party Assurance Policy


Breach or Incident Response Policy



Address State Data Privacy laws...
In MA, a Written Information Security
Plan is also required

<http://www.becker.edu/about/information-privacy/policies/>

Emerging Policies, and the Use of Position Papers at Brown

- Attribute Release Policy
 - Web Click-Through Agreements
 - Use of Skype
 - Multi-Function Network Devices
 - DNS Policy
 - Use of TOR
- 


Strategic Use of Audits

- Some are mandatory (credit cards, social security numbers)
- Data use / records management audits
- Visits, surveys, data element inventories...use them all
- Partner with Internal Audit for targeted areas of security and risk, and use the audit results to drive the security mission and reduce overall university risk

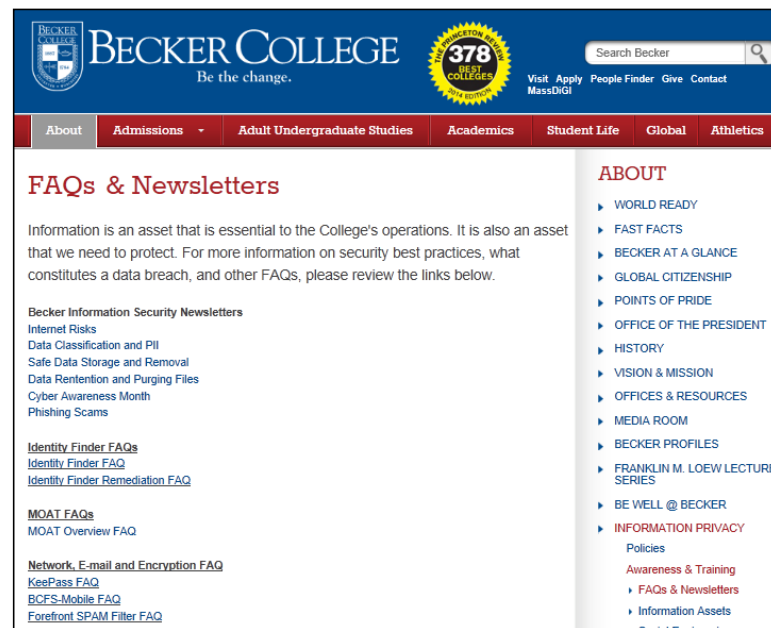
Implement Technology

- Firewalls
- DMZs
- Intrusion Detection/Prevention Systems
- Patch Management
- Database Activity Monitoring
- Employ DLP to find and monitor PII
 - Active DLP
 - Passive DLP
- Endpoint encryption
- Hard drive crusher
 - An amazing awareness tool, and excellent metrics to provide to the Risk Committee

Train and Educate End Users

- Mandatory for all employees (including student work studies)
 - Evolution of security threats
 - State & Federal regulations affecting security
 - Data classifications
 - Secure computing practices (Phishing)
 - Fines and reputational impact of breaches
- 

Provide Online User Resources




<http://www.becker.edu/about/information-privacy/awareness-training/faqs-and-newsletters-2/>

Brown's User Awareness Resources

- Morning Mail
- Brown Bag sessions (focus on “personal” use cases)
- Campus streaming services (Powerpoint, message boards, etc)
- “Securing the Human”
- Movie nights (free popcorn!)

Brown's Latest Resource: the "Phish Bowl"

INFORMATION FOR: CURRENT STUDENTS FACULTY STAFF FAMILIES ALUMNI FRIENDS & NEIGHBORS

 BROWN UNIVERSITY

Google Custom Search
Search Brown Search IT

About Brown Academics Admission Research Campus Life A TO Z INDEX PEOPLE DIRECTORY

INFORMATION TECHNOLOGY > PHISH BOWL

Information Technology

Home

About

Services

Get Support



Information Security

Announcements

SUBMIT HELP TICKET


CHAT WITH IT SUPPORT

IT Service Center
Brown University
M-F, 8am - 5pm
115 Waterman St., Lobby
Providence, RI
Phone 401-863-4357
help@brown.edu

Follow us:
 

PRINT THIS PAGE

Phish Bowl



The following emails are phishing attempts that have been reported by the Brown community. If you received one and do not see it here, please forward it to PhishBowl@brown.edu so it can be added.

If you received one already posted here, please report it as phishing to the Gmail team (from within the message, click on the down arrow to the right of the REPLY button and select "Report phishing") or simply delete it. More about phishing at brown.edu/go/phishing and What to do When You Spot a Phish.

PHISHING ALERT

School Receipt / Payment Receipt (Blackboard Learn)

Updated: Aug 18, 2014 - 1:45 pm


Content of Phishing email:

Forwarded message

From: Blackboard Learn Notifications <newsnotifications@learn.org>

Date: Mon, Aug 18, 2014 at 12:51 PM

Subject: School Receipt To:



Phishing Alerts

School Receipt / Payment Receipt (Blackboard Learn)

Updated: Aug 18 - 1:45 pm

Update Alert

Updated: Aug 18 - 1:20 pm

Message from Brown Information Security: Your email account ...

Updated: Aug 17 - 1:58 pm

Re-Validate Your School Mail Box

Updated: Aug 17 - 1:57 pm

Message from Brown Information Security...

Updated: Aug 16 - 11:33 am


Your Salary Raise Confirmation

Updated: Aug 15 - 12:52 pm

ERROR 20903

Updated: Aug 15 - 12:48 pm

Purchasing and contract reviews

- Establishing a strong and personal relationship with purchasing provides a lens in to the entire campus
 - Contracts now include language for security and privacy
 - Security can set the standards necessary for such areas as network copiers, shredding companies, click-through agreements, document management outsourcing, and others
 - As stated before, you should be reading items that pass through the IRB, the OSP, and the HPC
- 


Insurance and breach retainers

- Cyber Insurance is a risk management tool, via risk transference
- Be certain that you are agreeing to the right areas
- Many companies will now provide breach retainers with no money up front
 - Be certain to agree on the pricing for individual areas
 - Understand the response time
 - Sign off on the what determines when an incident becomes a breach

Incident response

- A foundational process for security management
- But also a key aid in risk management
- Make sure your process is documented
- Test regularly!
- Set “levels”, that determine what level of university involvement is needed
- Get inserted into the emergency management testing
- Have an annual update/refresh for those who were not effected in the previous 12-months

Concluding thoughts and recommendations

- Security Management is Risk Management
 - Our roles are less and less bits and bytes, and more and more policy, compliance and risk
 - Sound security strategies help in reducing risk to our institutions
 - Size, location, public/private, or Carnegie designation doesn't matter
 - Each of us has to find ways for the security mission to be part of all areas and every level of our organizations
 - The recommendations we've suggested are actionable, and have proven results
- 



PATTY PATRIA
CIO
BECKER COLLEGE
PPATRIA@BECKER.EDU



DAVID SHERRY
CISO
BROWN UNIVERSITY
DAVID_SHERRY@BROWN.EDU



