PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Welcome to

PES University

Bengaluru

Disclaimer

- ☞ *This presentation is purely educational.*

- ☞ *The views expressed by the presenter is not representation of any organization.*
- ☞ *The views are based on professional experience of the presenter and no liability is accepted by the presenter in the event of any potential or perceived losses resulting from this presentation.*

General rules of engagement

Raise your hand

- if you have a Question

A note on security

- In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks.
- To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner.
- In particular, you will comply with all my instructions when doing the labs.
  - My instructions are in consonance with applicable laws of India and PES University policies.
  - If in any doubt, please consult your professor!
- Any violation is at **YOUR RISK!** And may result in severe consequences.

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

The Phoenix Project:

Remediation of a Cybersecurity Crisis at the University of Virginia

Learning Objectives

- ☞ Describe the technical, social, and financial challenges faced by a university dealing with a cyberattack.
- ☞ Evaluate UVA's planned approach for remediation, with particular emphasis on the Phoenix Project.
- ☞ Assess best practices for managing risks, stakeholders, communication, vendors, cybersecurity, and cyberattack remediation.
- ☞ Decide how to best evaluate the success of the Phoenix Project.
- ☞ Develop executable recommendations tied to UVA's unique situation (context and timing).

Agenda

- ☞ Background on UVa, IT and the CIO
- ☞ Cybersecurity Circa 2015
- ☞ The Phoenix Project
- ☞ Decision Point
- ☞ Epilogue

Background

The University of Virginia

- ☞ Research Intensive University
- ☞ Top-ranked public school
  - 22,000 students
  - 2,800 faculty
  - 10,000 full-time staff

Information Technology Services @ UVa

- ☞ Leader in IT services in higher education
- ☞ 240 employees
- ☞ $22.6 million dollar budget
- ☞ Managed core university services with serveral hundred servers for
  - HR
  - Student Information
  - Financial Information
  - And other data

Personnel

- ☞ Virginia Evans: CIO
  - CIO for 1 ½ years
  - 20 year experience managing IT and people
- ☞ Dana German: Senior Director for Strategic Projects and Initiatives
- ☞ Pat Hogan: Executive Vice President and COO

The University of Virginia, ITS and Virginia Evans

☞ A privately funded Public University

RANKINGS

#4 Best Public National University, 2021 *U.S. News & World Report*

#1 Best-Value College in Virginia, 2019 *Forbes*

#2 Best-Value Public University, 2020 *Money Magazine*

#1 Best-Value Public College, 2019 *Princeton Review*

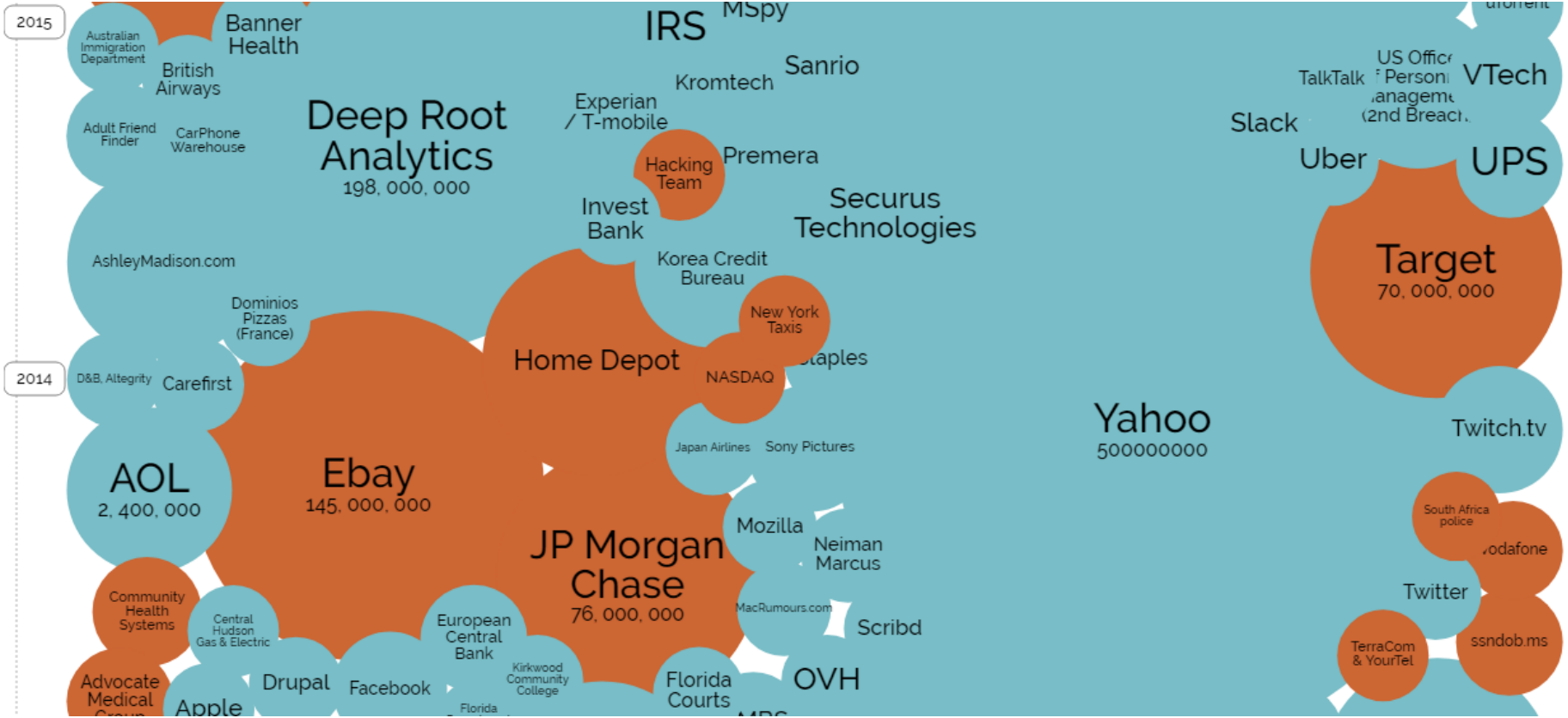
#7 Best-Value Public College, 2019 *Money Magazine*

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Cybersecurity Circa 2015

Mega Breaches in 2014 and 2015

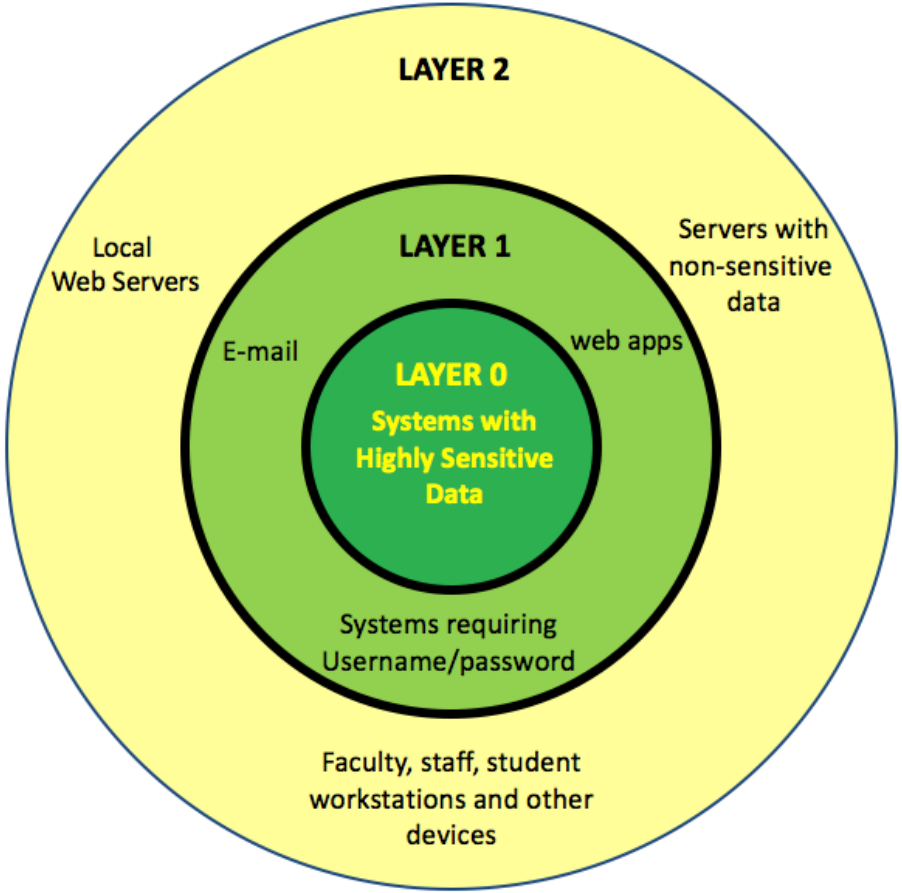


www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Cybersecurity Environment in 2015

Organization	Data compromised	How they got in	How long they went undetected	Why is it big?
US Government - Office of Personnel	22 million current and former federal employees	Using a contractor's stolen credentials	343 days	Seeking data on individuals for intelligence purposes.
Anthem	Personal information about more than 80 million people	Infecting websites that Anthem employees visited	Nine months	Largest number of records compromised in a healthcare network
Premera	PII, medical, and financial info for 11 million customers	Phishing	May 5, 2014 to Jan. 29, 2015	Likely same attackers as Anthem Attacks were discovered the same day.
IRS	330,000 taxpayers used to collect bogus refunds	Stolen credentials	Uncertain	The thieves collected tens of millions of dollars in fraudulent refunds

Cybersecurity Defense Model



Costs of deficient security

- When a breach occurs, it means your security failed. These questions will help qualify and quantify the cost of that failure:
- How efficient are you? How many false positives distract your security team and how many actual cyber security incidents do you uncover?
- Are you prioritizing correctly? How many cyber security incidents have an actual business impact and qualify for further investigation?
- Are you learning about your attackers? How many cyber security incidents can be fully investigated to determine threat actors and/or motives?
- What is your security protecting? How many of your solutions actively support a security policy or protect a quantifiable business asset?

Costs of breach consequences

- After a data breach, you need to figure out exactly what you will lose, how much, and what to do about it. These questions will help you calculate business losses:
- How much money will you lose based on information, such as intellectual property (IP) or personally identifiable information (PII), lost through the data breach?
- How much money will you lose to notification costs, lawsuits, fines, audits and brand damage when the data breach becomes public?
- How much time will it take to resolve the breach—to identify and address all affected systems, and respond to attacks?
- How much will you be fined if your security practices don't comply with security policies and requirements?

Cyber attacks exploit network vulnerabilities

- Advanced cyber attacks succeed because they are carefully planned, methodical and patient. Malware used in such attacks:
  - Settles into a system
  - Tries to hide
  - Searches out network vulnerabilities
  - Disables network security measures
  - Infects more endpoints and other devices
  - Calls back to command-and-control (CnC) servers
  - Waits for instructions to start extracting data from the network
- By the time most organizations realize they've suffered a data breach, they have actually been under attack for weeks, months, or even years.

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

The Phoenix Project

The Rise of Project Phoenix

- ☞ Mandiant on-site in 24-hours.

  (https://en.wikipedia.org/wiki/Mandiant)

- ☞ Omaha Team
  - Two members of the Board of Visitors
  - Senior communication personnel
  - General Counsel
  - Enterprise Risk Manager
  - CISO
  - Virginia Evans

Students reflect on Evan's Decisions:

- ☞ Create OMAHA Executive Team
- ☞ Dana as PM? Is she the right person given the critical and central role?
- ☞ Choice of Project Management Methodology?

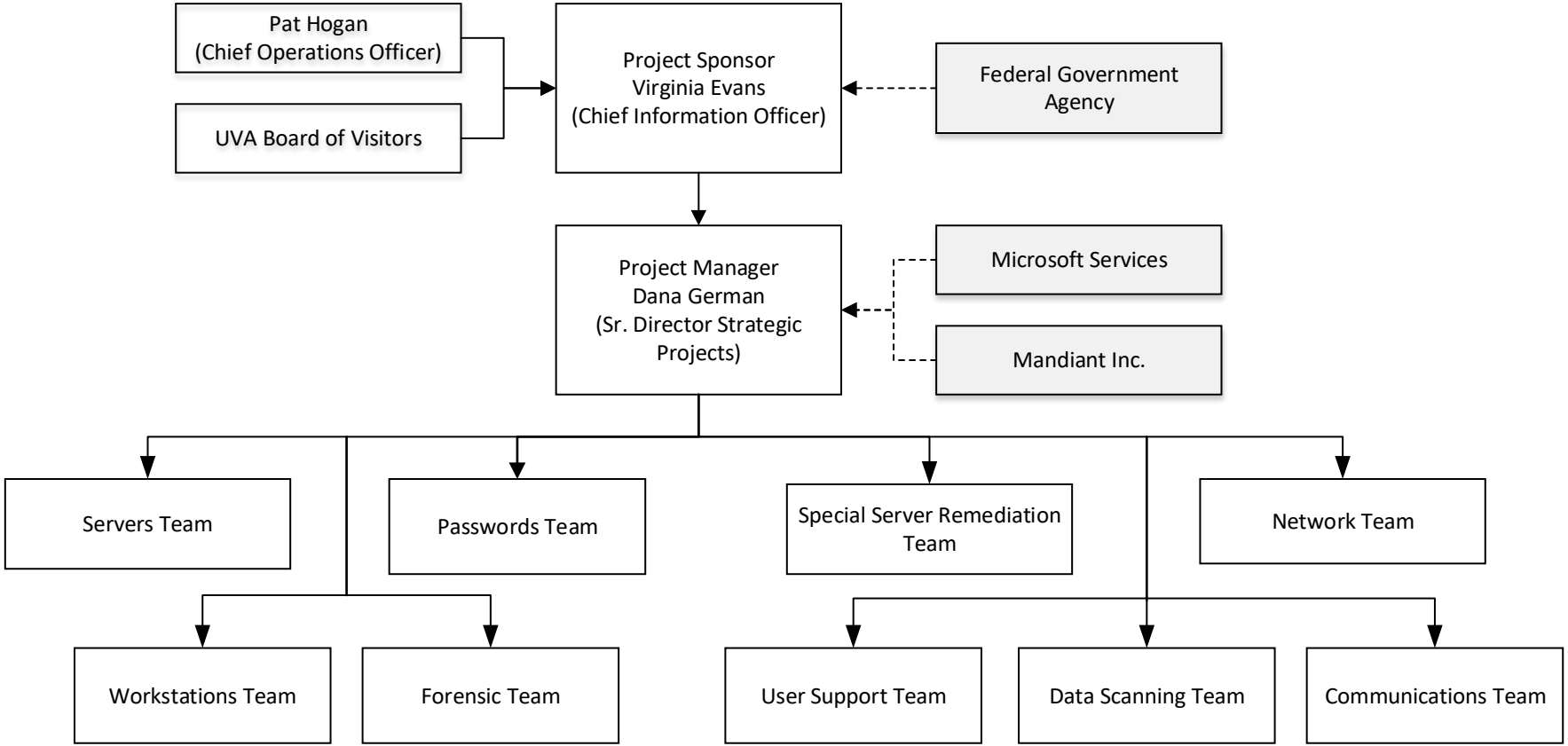
Project Phoenix – 5 High level objectives

- ☞ Determine the extent of the intrusion
- ☞ Develop a remediation plan
- ☞ Execute the remediation plan
- ☞ Harden UVA’s defenses
- ☞ Restore services

Organizing the Stealth Army

- ☞ Only critical personnel were “read-in”
- ☞ Used Shadow systems to communicate (e.g., Gmail)
- ☞ Requisitioned a building for the Stealth Army

Project Organization Chart



Project Phoenix Timeline

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Decision Point

Going Dark

- ☞ What methodology fits this project best (plan-based, agile, or a hybrid of the two)?
- ☞ What best practices should they employ?
  - risk management plan
  - development of a communication plan
  - cyberattack remediation
  - Methods of Procedures (MOP)
- ☞ What are the relevant metrics for evaluating project success in this situation?

Crisis Project Management

- How is this different than a regular project?
- What tools are necessary to succeed?
- How are the teams different?

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Epilogue

PM Method Decision

- ☞ The decision was to use a “hybrid” approach to the project.

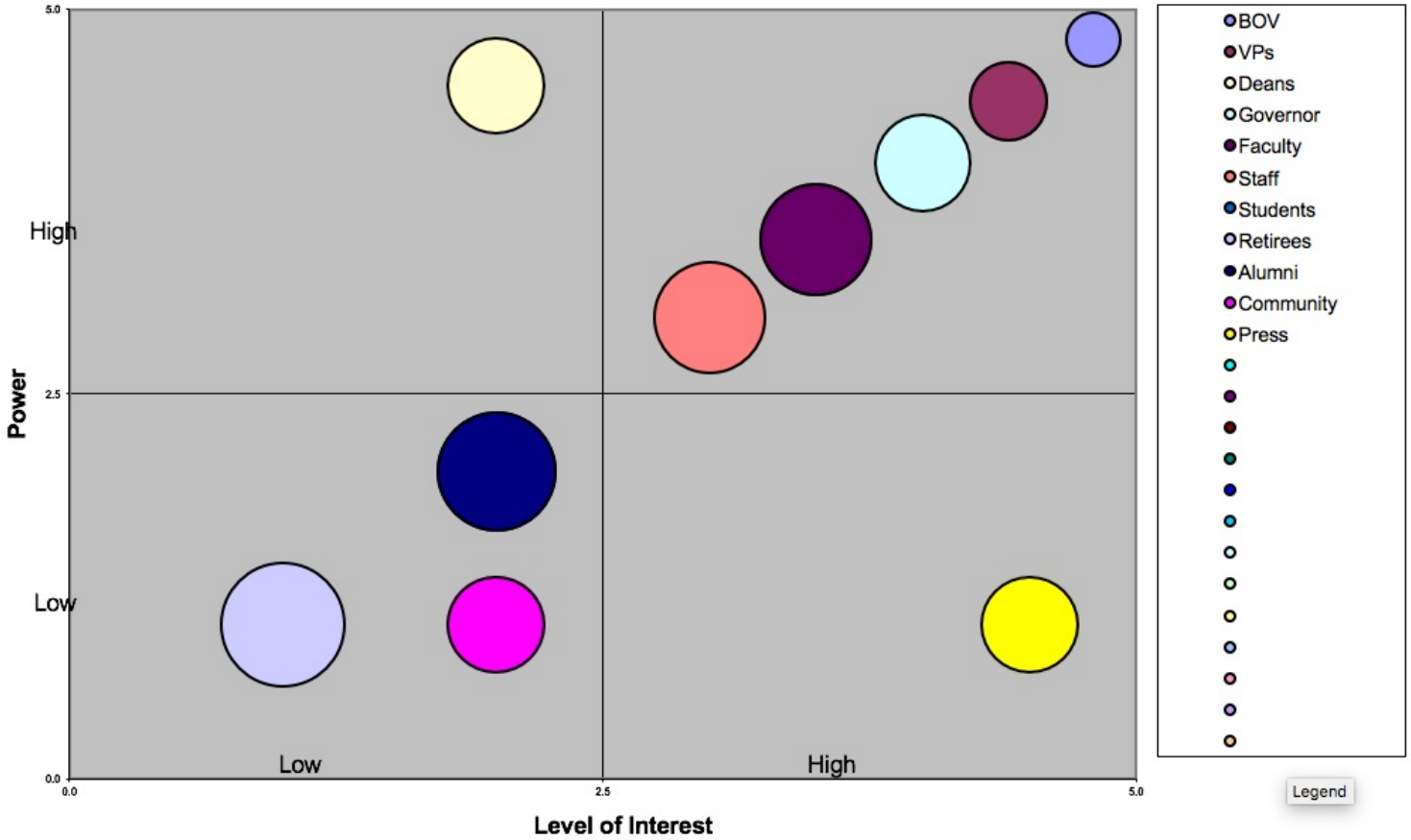
- ☞ While fundamentally it was a plan-based approach with a Gantt chart and traditional roles and responsibilities, the teams employed agile principles such as daily meetings (every morning at 9am).

Stakeholder Assessment

An effort was made to identify and manage all stake holder groups

- BOV
- Vice Presidents
- Deans
- Governor's office
- faculty
- staff
- students
- retirees
- alumni
- general public
- university community
- the press (e.g., the local newspaper and television stations)

Stakeholder Assessment



Risk Management Plan

- ☞ Approximately 20 risks were identified and assessed on two dimensions:
  - Impact
  - Probability

- ☞ Also included:
  - associated mitigation strategies
  - the owner of each risk

Example of Risk Register

Risk Assessment

Risk Number	Risk Status	Date Identified	Risk Description	Impact (1-4)	Probability (1-4)	Risk Factor (I*P)	Mitigation Strategy/Status	Owner	Next Review or Expected Mitigation Date
1	Retired	22-Jul-15	Security compromise becomes public before July 31st -- before mitigation is finalized and verified with Microsoft and Mandiant.	4	3	12	Whack-a-mole and monitor very closely. Bring in Mandiant and Microsoft ASAP. (We are not ready to scramble to remediate today!)		13-Aug-15
2	Retired	22-Jul-15	Security compromise becomes public after July 31st -- after mitigation finalized but before planned communication date/time.	1	2	2	Go dark and have an intense review before beginning to execute communication plan. (Each day beyond August 3rd, situation should gradually improve and risk will diminish.)		14-Aug-15

Communication Plan

☞ The project team developed an in-depth communication plan that detailed:

- The timing
- Audience
- Message
- Mechanism/medium
- Responsibility.

Example Communication Plan

Date	Time	Audience	Message	Mechanism	Assigned To	Status
Pre- "Go Dark"						
8/14	Morning	**Phoenix Project Team**	Where to direct inquiries	Project email accounts		
	4:00-5:00 PM	**Board of Visitors, Deans, VPs, Governor's Office**	Script composed	Phone calls		
	4:45 PM	**UVA's Local Support Personnel**	Alert to check its.virginia.edu after 5 PM	Email		
	4:55 PM	**University Community with a cc to Governor Paul Regan and AG's office**	FAQs, when things come back up, this is what you need to do (link to its.virginia.edu).	Emergency mass mail & mass mail		
		Governor Paul Regan	General letter with FAQs	Email		
		Attorney General's office	General letter with FAQs	Email		

“Go Bright” Communication Plan

4:00pm:

Phone calls to VIPs

4:45pm:

Email to Network Admin

4:55pm:

Mass email with COO MEssage

5:01pm:

virginia.edu & ITSWeb change

Text

Just after 5pm:

News release

Tweet by UVa

1hr prior to go light:

Email to Network

Just after go light:

Mass mail

Text message

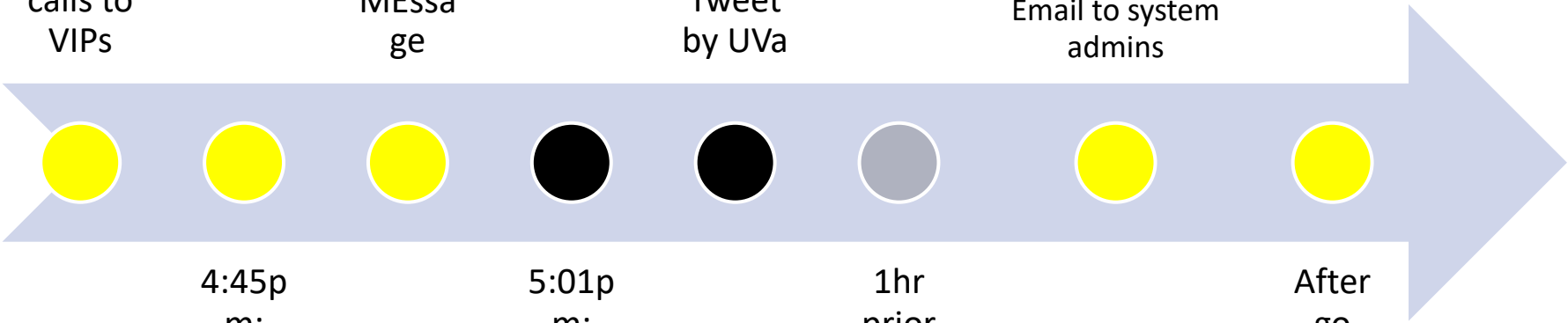
virginia.edu & ITSWeb up

Tweet by Uva

Email to system admins

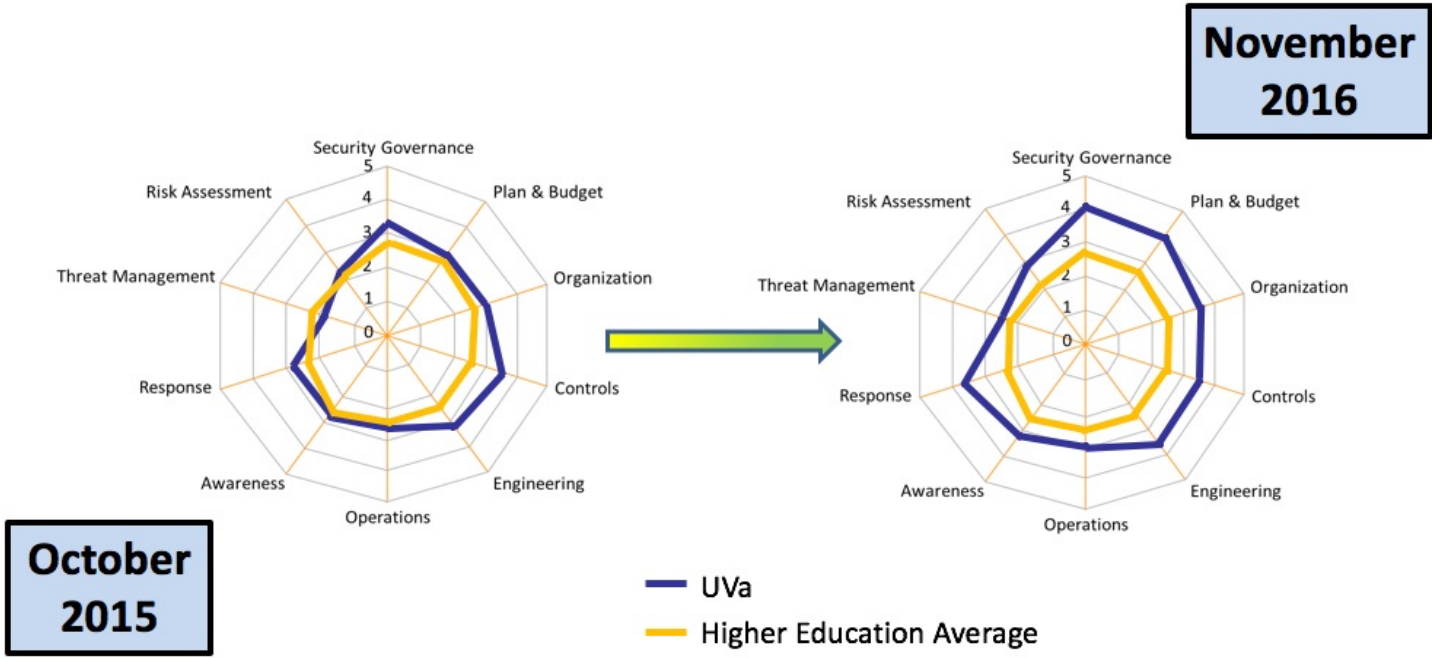
After go light:

Email password reset remind



Cyber Attack Remediation Plan – A Successful Project

Security Benchmark was undertaken by Gartner Consulting



Significant Improvement in First Year+; Surpassing others in Higher Ed

Project Status

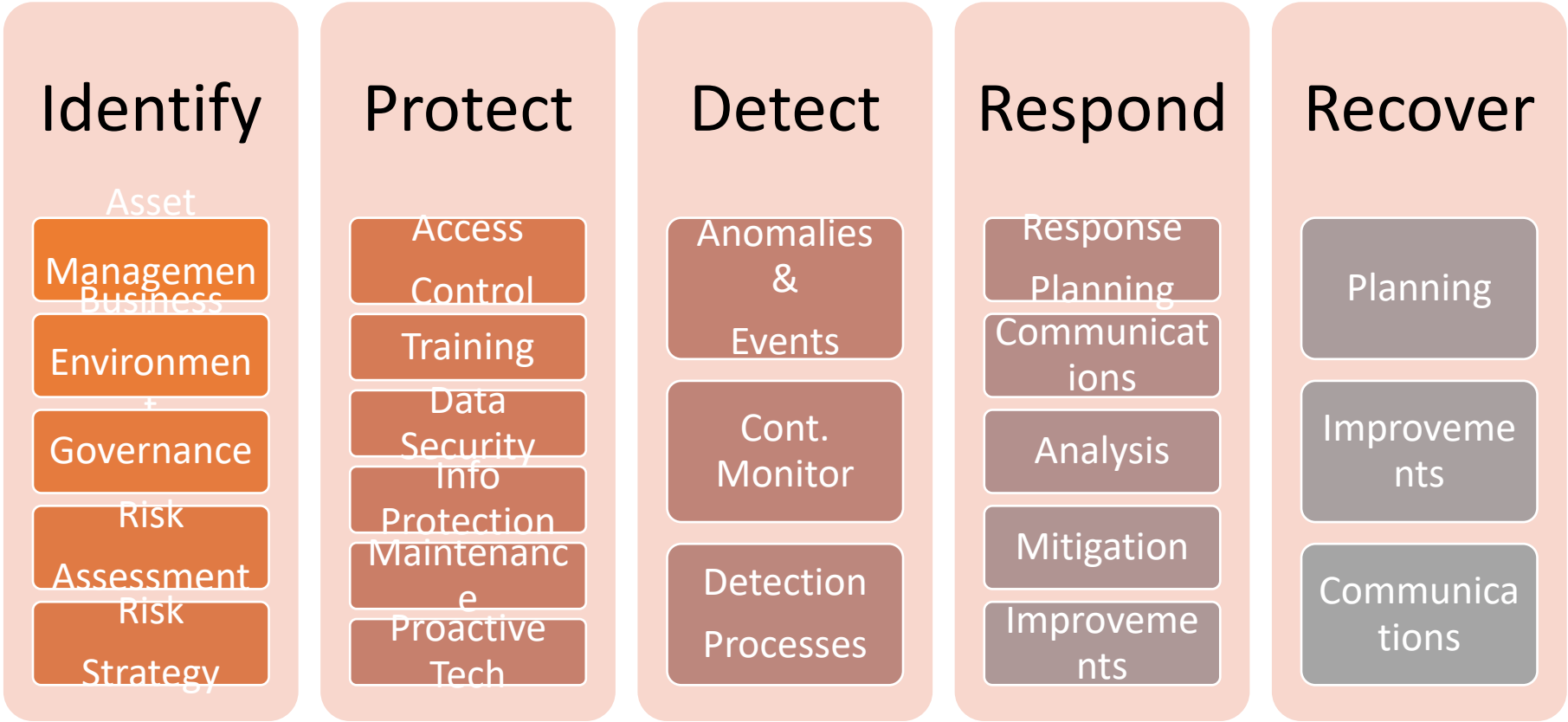
- ☞ Time – Project finished on schedule
- ☞ Cost – well with in cost compared with similar work elsewhere – 2 MUSD, 12,000 person hours
- ☞ Scope – All 5 high level objectives were achieved
- ☞ Use / Adoption – An all-NEW password system was implemented, and the changeover was much smoother than anticipated
- ☞ Uva brand and reputation were protected from further damage
- ☞ Lots of learnings and takeaways

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Appendices

NIST Cyber Security Framework



Aug. 15, 2015

Outdoors: Five things to love about Douthat State Park, located near the West Virginia border C1

The Daily Progress

Charlottesville, Virginia | DailyProgress.com

Home delivery price: 40¢ | 75¢

WEATHER High: 88° Low: 66° Forecast: A2

SATURDAY, AUGUST 15, 2015

UVa targeted by cyberattack

Officials: Systems, including email, inaccessible until upgrade is completed possibly on Sunday

BY DEAN SEAL

The University of Virginia shut down access to many of its information technology systems Friday in response to a cyberattack that originated in China, the university announced in a release.

After receiving an alert from federal authorities, the university confirmed June 11 that "sophisticated attackers" from China had illegally accessed portions of UVa's IT systems. The university quickly tapped cyber security firm Mandiant to identify the nature of the attack and work to correct it. Mandiant rose to prominence in 2013 for releasing documentation of cyberattacks on the U.S. by the Chinese military.

The attack specifically targeted the email accounts of two employees whose work is connected with China, university officials told The Daily Progress. However, the identities and departments of those employees have not been released. They remain employed at the university, officials said Friday.

DAILY PROGRESS FILE

The University of Virginia waited two months to announce the breach to "best protect against future attacks" by being "confident that notification would not jeopardize ... efforts to secure systems," officials said Friday.

Forensic examination has indicated that personal information, including Social Security numbers, banking information and personal health records, was not accessed during the breach. There is also no evidence that any of the university's research or similarly sensitive information was accessed, the university said in a release.

The university waited two months to announce the breach to "best protect against future attacks" by being "confident that notification would not jeopardize ... efforts to secure systems," officials said in a news release Friday.

"It is important that the hackers remain unaware of our action to investigate this event and protect against it," the university's release states. "If the university had not taken this course of action, the situation could have worsened."

See **ATTACK**, Page A6

FAQ: WHAT YOU NEED TO KNOW ABOUT THE UVA CYBERATTACK

» What happened? Sophisticated attackers from China hacked portions of the university's information technology systems.

» Who was targeted? Two UVa employees whose work was about China were specifically targeted in the attack.

» What was not targeted? No personally identifiable information or personal health information was accessed by the attackers.

» Why is UVa email down? UVa is upgrading its IT security systems. Many university systems, including email accounts, will be inaccessible until Sunday evening.

» For full FAQ, see **Page A6.**

Aug. 17, 2015

Prep football: Louisa eyes playoff run after Fischer's first season back as coach B1

The Daily Progress

Charlottesville, Virginia | DailyProgress.com

Home delivery price: 40¢ | 75¢

WEATHER High: 91° Low: 70° Forecast: A2

MONDAY, AUGUST 17, 2015

UNIVERSITY OF VIRGINIA

Computer system restored after attack

Sullivan: Board of Visitors' goal is 500 new faculty hires over 5 years

BY DEREK QUIZON

The University of Virginia's computer network was restored Sunday afternoon, two days after officials shut it down in response to cybersecurity threats.

The attack, thought to have originated in China, targeted the personal email accounts of two university employees. UVa administrators say the hackers did not obtain any sensitive personal information or research data, but shut down much of the university's network on Friday afternoon.

The university is currently making adjustments to the password change program to guard against further breaches, said UVa Chief Operating Officer Patrick D. Hogan.

"We're running through all sorts of testing and routines right now," Hogan told members of the Board of Visitors on Sunday at their first meeting of the new academic year.

"We were quite fortunate in this incident," Hogan added. "We're not aware of any personal information or research data that was stolen or lost."

The administration announced that systems were back online just before 4 p.m. Sunday. The message urges students, faculty and staff members to change their passwords.

Anyone seeking further information can call the UVa Help

See UVA, Page A5

LOUISA

Not lost to history

JULIAN BOND: 1940-2015

Civil rights icon a UVa professor

Ex-NAACP leader taught for 20 years before departing history department

THE ASSOCIATED PRESS

ATLANTA — Julian Bond's life traced the arc of the civil rights movement, from his efforts as a militant young man to start a student protest group, through a long career in politics and his leadership of the NAACP almost four decades later.

Year after year, the calm, telegenic Bond was one of the nation's most poetic voices for equality, inspiring fellow activists with his words in the 1960s and

Bond, a member of the Corcoran Department of History, retired from UVa in 2012. The university established an endowed chair in his honor.

UVa President Teresa A. Sullivan called for a moment of silence in Bond's memory at Sunday's Board of Visitors meeting. Sullivan said Bond was "very important to thousands of students to whom he taught the history of civil rights — something he lived as well as taught."

Presented to all members of the Project Phoenix team after completion of the project.

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Assignment

Assignment Questions

1. Describe the role of Information Technology Services (ITS) in fulfilling UVA's mission.
2. What attracts cyber attackers to universities?
3. What are the most common attack methods and approaches for mitigating those attacks?
4. Describe each of the five objectives of the Phoenix Project. What level of effort would be required to accomplish these objectives?

Assignment Questions

5. Describe the various internal and external stakeholders associated with the Phoenix Project. How would you recommend the project team communicate with each stakeholder group?
6. Identify the key risks inherent to this project. How would you recommend the team manage these risks?
7. When and how should the success of the Phoenix Project be evaluated?

Suggested reading for todays class

- Dara Kerr, “Cyberattack on Penn State Exposes Passwords of 18K People,” CNET, May 15, 2015,
  - ☞ https://www.cnet.com/news/penn-state-cyberattack-exposes-passwords-from-18k-people/ (accessed Sept. 14, 2017).

- AnthonydeBruyn,“U.VA.RespondstoCyberAttackonPortionsofITSystems,”by,*UVAToday*, August 14, 2015.

- R. Ryan Nelson, “IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices,” *MIS Quarterly Executive* 6, no. 2 (2007): 67–78.

- R. Ryan Nelson, “Project Retrospectives: Evaluating Project Success, Failure, and Everything in Between,” *MIS Quarterly Executive* 4, no. 3 (2005): 361–372.

Thank You!

- ☞ Thank You!

Email: Prasad.honnavalli@gmail.com

Call: +91 998 099 3885

Director,

Centre for Information Security, Forensics and Cyber Resilience (C-ISFCR)

Professor,

Computer Science and Engineering

PES University, Bangalore

Follow us at:

https://isfcr.pes.edu

https://www.linkedin.com/company/isfcr

@isfcr.pesu

PESU Center for Information Security, Forensics and Cyber Resilience

PESU Center for Internet of Things