Unit - #1

MIS5214 – Security Architecture

Agenda

- Welcome and Introductions
- Course Introduction Goals
- Introductory Terminology
- The Threat Environment
- Next Week…

Course Goals – Security Architecture

Learn about how organizations

- Align their IT security capabilities with their business goals and strategy
- Plan, design and develop enterprise security architectures
- Assess IT system security architectures and capabilities

Objectives

1. Learn key Enterprise Security Architecture concepts
2. Develop an understanding of contextual, conceptual, logical, component, and physical levels of security architectures and how they relate to one another
3. Learn how security architectures are planned, designed and documented
4. Gain an overview of how security architectures are evaluated and assessed
5. Gain experience working as part of a team, developing and delivering a professional presentation

Course Web Site

https://community.mis.temple.edu/mis5214sec004spring2020/welcome-to-security-architecture/

Instructor

HOMEPAGE | INSTRUCTOR | SYLLABUS | SCHEDULE | DELIVERABLES | HARVARD COURSEPACK | GRADEBOOK

Fox School of Business
TEMPLE UNIVERSITY

ABOUT AWARDS BIOGRAPHY EDUCATION POSITIONS PUBLICATIONS SAMPLE PAGE SYSTEMS

David Lanter

Director, Master of Science – IT Auditing & Cyber Security

Edit

FOX MIS Faculty/Staff

Edit

Connect with Me

Edit

Contact Information

209C Speakman Hall | 1810 N. 13th Street Philadelphia PA 19122 | david.lanter@temple.edu | T 215.204.3044

Edit

Office Hours

Wednesdays 1-3 PM, and before and after classes and by appointment.

Edit

DAVID LANTER PhD GISP CISA

Director – Information Technology Auditing and Cyber Security (**ITACS**) Master of Science program

Management Information Systems

Fox School of Business, Temple University
209C Speakman Hall
1810 North 13th Street
Philadelphia, PA 19122-6083

Phone: +1.215.204.3077

Email: David.Lanter@Temple.edu

ABOUT

A pioneering inventor of data provenance/lineage metadata and geospatial data management and quality assurance, Prof. Lanter was vice president at CDM Smith where he routinely led teams of software engineers, computer scientists, data specialists, and subject matter experts in designing, developing and securing high-performance applications, decision support systems, and enterprise data architectures for public and private sector organizations from the international to the municipal level. As research director at Rand McNally, Prof. Lanter led global and domestic data research and development teams; As software design engineer at Microsoft – Prof. Lanter led GeoModeling quality assurance for the firm's geography products; and president of Geographic Designs Inc. – where he developed commercial off the shelf and custom artificial intelligence metadata processing capabilities for government agencies, utility and private organizations enabling them to visualize and analyze big datasets and manage quality in their enterprise information systems. As a systems analyst at Grumman Data Systems he designed a reusable software library for cartographic applications for tactical and strategic systems of the U.S. Air Force. At University of California in Santa Barbara, he taught Geographic Information Systems, cartographic design and production, and applications programming.

RECENT PUBLICATIONS

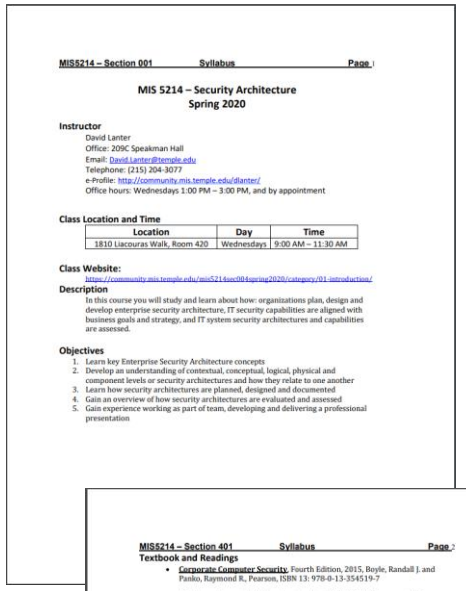
Lanter, D.P. and R. Essinger, 2017, "**User Centered Design**", in **International Encyclopedia of Geography: People, the Earth, Environment and Technology**, New York: John Wiley and Sons.

Lanter, D.P., Durden, S., Baker, C., and Dunning, C.M., 2017, "**Social Vulnerability eXplorer (SV-X)**", in **Proceedings of the Coastal Structures & Solutions to Coastal Disasters Joint Conference; Coasts, Oceans, Ports and Rivers Institute (COPRI)**; American Society of Civil Engineers.

Tullis, J.A., J.D. Cothren, D.P. Lanter, X. Shi, W.F. Limp, R.F. Linck, S.G. Young and T. Alsumaiti, 2016, "**Geoprocessing, Workflows, and Provenance**", in **Remote Sensing Handbook: Remotely Sensed Data Characterization, Classification, and Accuracies**, edited by P. Thenkabail, Vol. 1., pp. 401-422, Boca Raton, FL: CRC Press.

Syllabus

HOMEPAGE | INSTRUCTOR | SYLLABUS | SCHEDULE | DELIVERABLES | HARVARD COURSEPACK | GRADEBOOK



MIS5214 – Section 001 Syllabus Page 1

MIS 5214 – Security Architecture
Spring 2020

Instructor

David Lanter
Office: 209C Speakman Hall
Email: David.Lanter@temple.edu
Telephone: (215) 204-3077
e-Profile: http://community.mis.temple.edu/dlanter/
Office hours: Wednesdays 1:00 PM – 3:00 PM, and by appointment

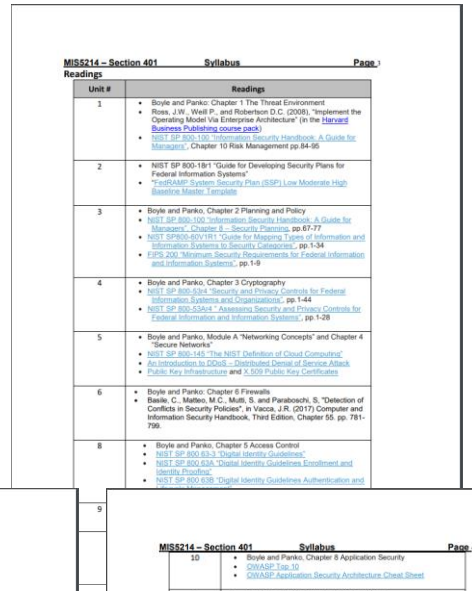
Class Location and Time

Location	Day	Time
1810 Liacouras Walk, Room 420	Wednesdays	9:00 AM – 11:30 AM

Class Website:
https://community.mis.temple.edu/mis5214sec004spring2020/category/01-introduction/

Description
In this course you will study and learn about how: organizations plan, design and develop enterprise security architecture, IT security capabilities are aligned with business goals and strategy, and IT system security architectures and capabilities are assessed.

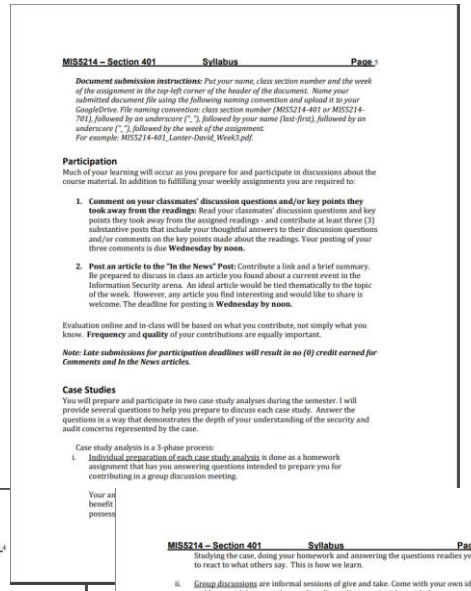
Objectives
1. Learn key Enterprise Security Architecture concepts
2. Develop an understanding of contextual, conceptual, logical, physical and component levels or security architectures and how they relate to one another
3. Learn how security architectures are planned, designed and documented
4. Gain an overview of how security architectures are evaluated and assessed
5. Gain experience working as part of team, developing and delivering a professional presentation



MIS5214 – Section 401 Syllabus Page 3

Readings

Unit #	Readings
1	• Boyle and Panko: Chapter 1 The Threat Environment • Rose, J.W., Weill P., and Robertson D.C. (2008), "Implement the Operating Model Via Enterprise Architecture" (in the Harvard Business Publishing course pack) • NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 10 Risk Management pp.84-95
2	• NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems" • "FedRAMP System Security Plan (SSP) Low Moderate High Baseline Master Template"
3	• Boyle and Panko, Chapter 2 Planning and Policy • NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 8 – Security Planning, pp.67-77 • NIST SP800-60V1R1 "Guide for Mapping Types of Information and Information Systems to Security Categories", pp.1-34 • FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems", pp.1-9
4	• Boyle and Panko, Chapter 3 Cryptography • NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations", pp.1-44 • NIST SP 800-53Ar4 " Assessing Security and Privacy Controls for Federal Information and Information Systems", pp.1-28
5	• Boyle and Panko, Module A "Networking Concepts" and Chapter 4 "Secure Networks" • NIST SP 800-145 "The NIST Definition of Cloud Computing" • An Introduction to DDoS – Distributed Denial of Service Attack • Public Key Infrastructure and X.509 Public Key Certificates
6	• Boyle and Panko: Chapter 6 Firewalls • Basile, C., Matteo, M.C., Mutti, S. and Paraboschi, S. "Detection of Conflicts in Security Policies", in Vacca, J.R. (2017) Computer and Information Security Handbook, Third Edition, Chapter 55. pp. 781-799.
8	• Boyle and Panko, Chapter 5 Access Control • NIST SP 800 63-3 "Digital Identity Guidelines" • NIST SP 800 63A "Digital Identity Guidelines Enrollment and Identity Proofing" • NIST SP 800 63B "Digital Identity Guidelines Authentication and
9	



MIS5214 – Section 401 Syllabus Page 5

Document submission instructions: *Put your name, class section number and the week of the assignment in the top-left corner of the header of the document. Name your submitted document file using the following naming convention and upload it to your GoogleDrive. File naming convention: class section number (MIS5214-401 or MIS5214-701), followed by an underscore ("_"), followed by your name (last-first), followed by an underscore ("_"), followed by the week of the assignment.*
For example: MIS5214-401_Lanter-David_Week3.pdf.

Participation
Much of your learning will occur as you prepare for and participate in discussions about the course material. In addition to fulfilling your weekly assignments you are required to:

1. **Comment on your classmates' discussion questions and/or key points they took away from the readings:** Read your classmates' discussion questions and key points they took away from the assigned readings - and contribute at least three (3) substantive posts that include your thoughtful answers to their discussion questions and/or comments on the key points made about the readings. Your posting of your three comments is due **Wednesday by noon.**
2. **Post an article to the "In the News" Post:** Contribute a link and a brief summary. Be prepared to discuss in class an article you found about a current event in the Information Security arena. An ideal article would be tied thematically to the topic of the week. However, any article you find interesting and would like to share is welcome. The deadline for posting is **Wednesday by noon.**

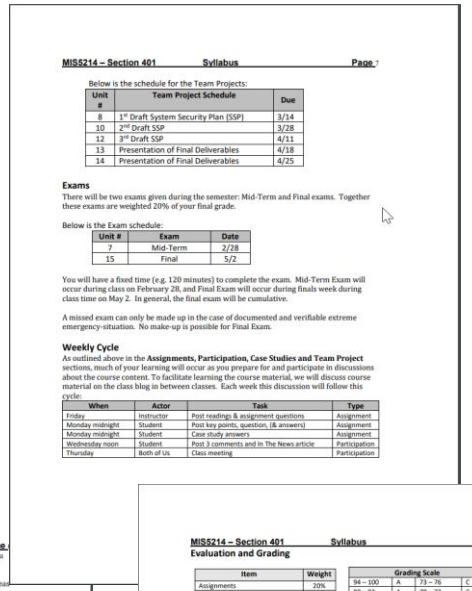
Evaluation online and in-class will be based on what you contribute, not simply what you know. **Frequency** and **quality** of your contributions are equally important.

Note: Late submissions for participation deadlines will result in no (0) credit earned for Comments and In the News articles.

Case Studies
You will prepare and participate in two case study analyses during the semester. I will provide several questions to help you prepare to discuss each case study. Answer the questions in a way that demonstrates the depth of your understanding of the security and audit concerns represented by the case.

Case study analysis is a 3-phase process:
i. Individual preparation of each case study analysis is done as a homework assignment that has you answering questions intended to prepare you for contributing in a group discussion meeting.

Your ar
benefit
possess



MIS5214 – Section 401 Syllabus Page 7

Below is the schedule for the Team Projects:

Unit #	Team Project Schedule	Due
8	1st Draft System Security Plan (SSP)	3/14
10	2nd Draft SSP	3/28
12	3rd Draft SSP	4/11
13	Presentation of Final Deliverables	4/18
14	Presentation of Final Deliverables	4/25

Exams
There will be two exams given during the semester: Mid-Term and Final exams. Together these exams are weighted 20% of your final grade.

Below is the Exam schedule:

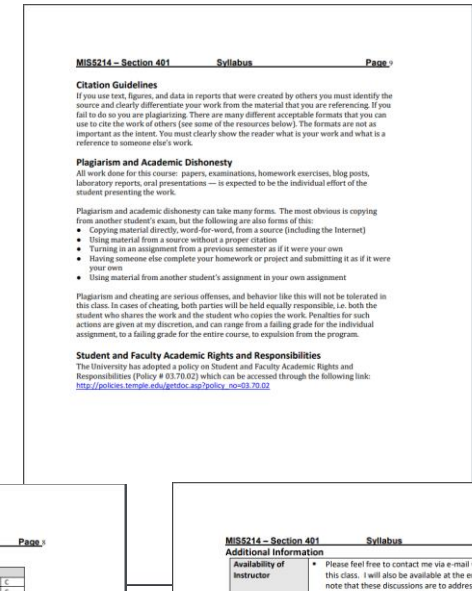
Unit #	Exam	Date
7	Mid-Term	2/28
15	Final	5/2

You will have a fixed time (e.g. 120 minutes) to complete the exam. Mid-Term Exam will occur during class on February 28, and Final Exam will occur during finals week during class time on May 2. In general, the final exam will be cumulative.

A missed exam can only be made up in the case of documented and verifiable extreme emergency-situation. No make-up is possible for Final Exams.

Weekly Cycle
As outlined above in the **Assignments, Participation, Case Studies and Team Project** sections, much of your learning will occur as you prepare for and participate in discussions about the course content. To facilitate learning the course material, we will discuss course material on the class blog in between classes. Each week this discussion will follow this cycle:

When	Actor	Task	Type
Friday	Instructor	Post readings & assignment questions	Assignment
Monday midnight	Student	Post key points, question, (& answers)	Assignment
Monday midnight	Student	Case study answers	Assignment
Wednesday noon	Student	Post 3 comments and In The News article	Participation
Thursday	Both of Us	Class meeting	Participation



MIS5214 – Section 401 Syllabus Page 9

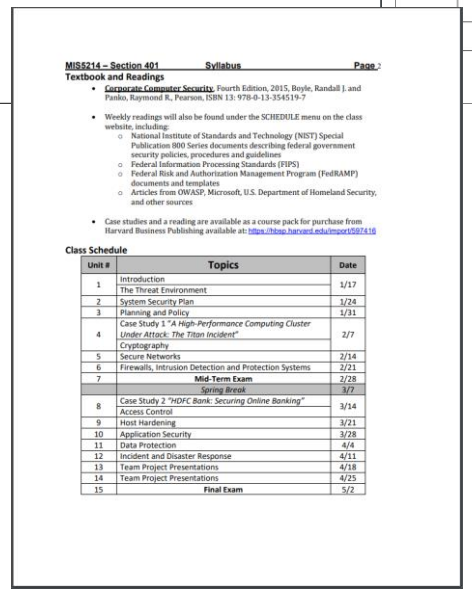
Citation Guidelines
If you use text, figures, and data in reports that were created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others (see some of the resources below). The formats are not as important as the intent. You must clearly show the reader what is your work and what is a reference to someone else's work.

Plagiarism and Academic Dishonesty
All work done for this course: papers, examinations, homework exercises, blog posts, laboratory reports, oral presentations — is expected to be the individual effort of the student presenting the work.

Plagiarism and academic dishonesty can take many forms. The most obvious is copying from another student's exam, but the following are also forms of this:
- Copying material directly, word-for-word, from a source (including the Internet)
- Using material from a source without a proper citation
- Turning in an assignment from a previous semester as if it were your own
- Having someone else complete your homework or project and submitting it as if it were your own
- Using material from another student's assignment in your own assignment

Plagiarism and cheating are serious offenses, and behavior like this will not be tolerated in this class. In cases of cheating, both parties will be held equally responsible, i.e. both the student who shares the work and the student who copies the work. Penalties for such actions are given at my discretion, and can range from a failing grade for the individual assignment, to a failing grade for the entire course, to expulsion from the program.

Student and Faculty Academic Rights and Responsibilities
The University has adopted a policy on Student and Faculty Academic Rights and Responsibilities (Policy # 03.70.02) which can be accessed through the following link:
http://policies.temple.edu/getdoc.asp?policy_no=03.70.02



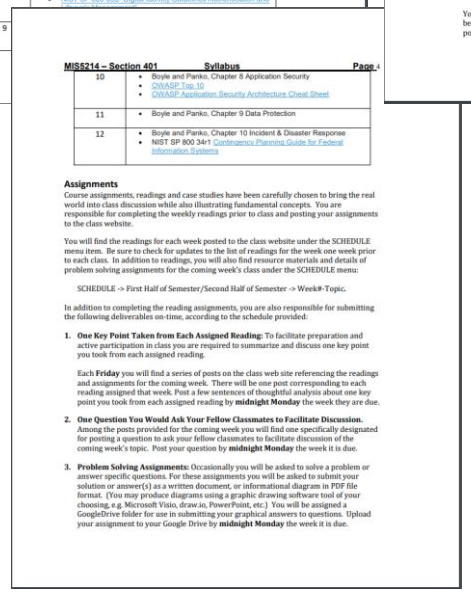
MIS5214 – Section 401 Syllabus Page 2

Textbook and Readings

- **Corporate Computer Security**, Fourth Edition, 2015, Boyle, Randall J. and Panko, Raymond R., Pearson, ISBN 13: 978-0-13-354519-7
- Weekly readings will also be found under the SCHEDULE menu on the class website, including:
  - National Institute of Standards and Technology (NIST) Special Publication 800 Series documents describing federal government security policies, procedures and guidelines
  - Federal Information Processing Standards (FIPS)
  - Federal Risk and Authorization Management Program (FedRAMP) documents and templates
  - Articles from OWASP, Microsoft, U.S. Department of Homeland Security, and other sources
- Case studies and a reading are available as a course pack for purchase from Harvard Business Publishing available at: https://hbsp.harvard.edu/import/597416

Class Schedule

Unit #	Topics	Date
1	Introduction The Threat Environment	1/17
2	System Security Plan	1/24
3	Planning and Policy	1/31
4	Case Study 1 "*A High-Performance Computing Cluster Under Attack: The Titan Incident*" Cryptography	2/7
5	Secure Networks	2/14
6	Firewalls, Intrusion Detection and Protection Systems	2/21
7	**Mid-Term Exam**	2/28
	Spring Break	3/7
8	Case Study 2 "*HDFC Bank: Securing Online Banking*" Access Control	3/14
9	Host Hardening	3/21
10	Application Security	3/28
11	Data Protection	4/4
12	Incident and Disaster Response	4/11
13	Team Project Presentations	4/18
14	Team Project Presentations	4/25
15	**Final Exam**	5/2



MIS5214 – Section 401 Syllabus Page 4

10	• Boyle and Panko, Chapter 8 Application Security • OWASP Top 10 • OWASP Application Security Architecture Cheat Sheet	
11	• Boyle and Panko, Chapter 9 Data Protection	
12	• Boyle and Panko, Chapter 10 Incident & Disaster Response • NIST SP 800 34r1 Contingency Planning Guide for Federal Information Systems	

Assignments
Course assignments, readings and case studies have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts. You are responsible for completing the weekly readings prior to class and posting your assignments to the class website.

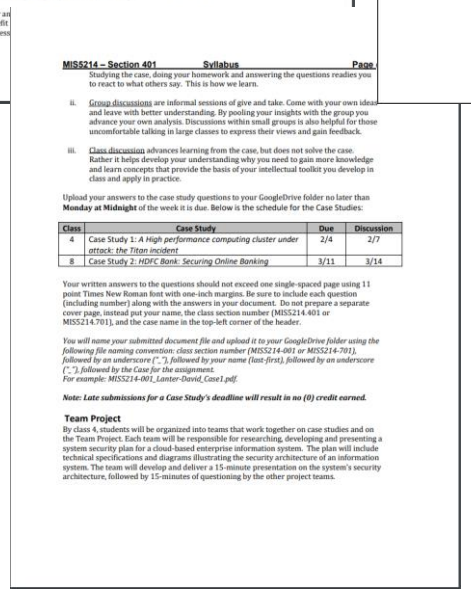
You will find the readings for each week posted to the class website under the SCHEDULE menu item. Be sure to check for updates to the list of readings for the week one week prior to each class. In addition to readings, you will also find resource materials and details of problem solving assignments for the coming week's class under the SCHEDULE menu:

SCHEDULE -> First Half of Semester/Second Half of Semester -> Week#-Topic.

In addition to completing the reading assignments, you are also responsible for submitting the following deliverables on-time, according to the schedule provided:

1. **One Key Point Taken from Each Assigned Reading:** To facilitate preparation and active participation in class you are required to summarize and discuss one key point you took from each assigned reading.

   Each **Friday** you will find a series of posts on the class web site referencing the readings and assignments for the coming week. There will be one post corresponding to each reading assigned that week. Post a few sentences of thoughtful analysis about one key point you took from each assigned reading by **midnight Monday** the week they are due.
2. **One Question You Would Ask Your Fellow Classmates to Facilitate Discussion.** Among the posts provided for the coming week you will find one specifically designated for posting a question to ask your fellow classmates to facilitate discussion of the coming week's topic. Post your question by **midnight Monday** the week it is due.
3. **Problem Solving Assignments:** Occasionally you will be asked to solve a problem or answer specific questions. For these assignments you will be asked to submit your solution or answer(s) as a written document, or informational diagram in PDF file format. (You may produce diagrams using a graphic drawing software tool of your choosing, e.g. Microsoft Visio, draw.io, PowerPoint, etc.) You will be assigned a GoogleDrive folder for use in submitting your graphical answers to questions. Upload your assignment to your Google Drive by **midnight Monday** the week it is due.



MIS5214 – Section 401 Syllabus Page

Studying the case, doing your homework and answering the questions readies you to react to what others say. This is how we learn.

ii. Group discussions are informal sessions of give and take. Come with your own ideas and leave with better understanding. By pooling your insights with the group you advance your own analysis. Discussions within small groups is also helpful for those uncomfortable talking in large classes to express their views and gain feedback.

iii. Class discussion advances learning from the case, but does not solve the case. Rather it helps develop your understanding why you need to gain more knowledge and learn concepts that provide the basis of your intellectual toolkit you develop in class and apply in practice.

Upload your answers to the case study questions to your GoogleDrive folder no later than **Monday at Midnight** of the week it is due. Below is the schedule for the Case Studies:

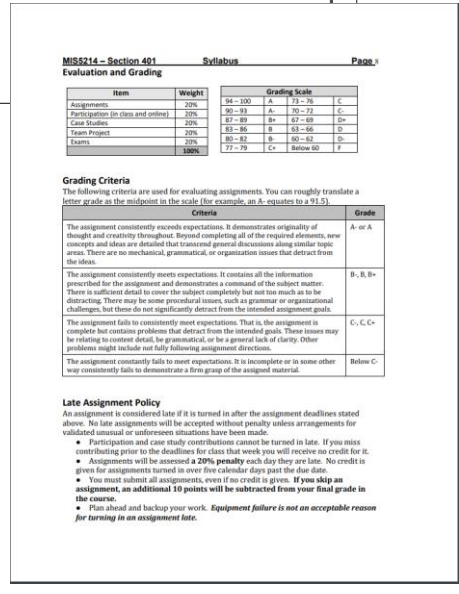
Class	Case Study	Due	Discussion
4	Case Study 1: *A High performance computing cluster under attack: the Titan incident*	2/4	2/7
8	Case Study 2: *HDFC Bank: Securing Online Banking*	3/11	3/14

Your written answers to the questions should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Be sure to include each question (including number) along with the answers in your document. Do not prepare a separate cover page, instead put your name, the class section number (MIS5214.401 or MIS5214.701), and the case name in the top-left corner of the header.

You will name your submitted document file and upload it to your GoogleDrive folder using the following file naming convention: class section number (MIS5214-001 or MIS5214-701), followed by an underscore ("_"), followed by your name (last-first), followed by an underscore ("_"), followed by the Case for the assignment.
For example: MIS5214-401_Lanter-David_Case1.pdf.

Note: Late submissions for a Case Study's deadline will result in no (0) credit earned.

Team Project
By class 4, students will be organized into teams that work together on case studies and on the Team Project. Each team will be responsible for researching, developing and presenting a system security plan for a cloud-based enterprise information system. The plan will include technical specifications and diagrams illustrating the security architecture of an information system. The team will develop and deliver a 15-minute presentation on the system's security architecture, followed by 15-minutes of questioning by the other project teams.



MIS5214 – Section 401 Syllabus Page 8

Evaluation and Grading

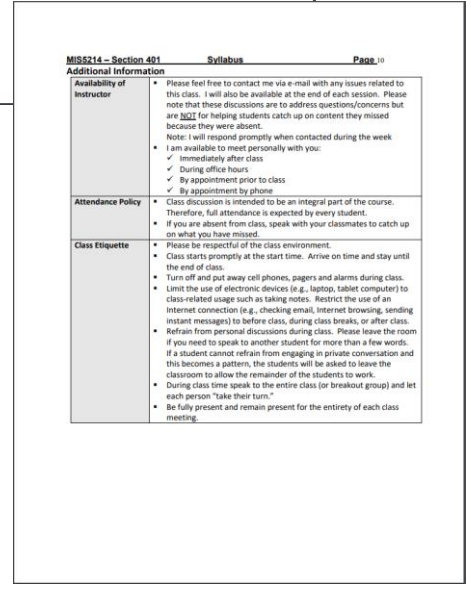
Item	Weight
Assignments	20%
Participation (in class and online)	20%
Case Studies	20%
Team Project	20%
Exams	20%
	100%

Grading Scale			
94 – 100	A	73 – 76	C
90 – 93	A-	70 – 72	C-
87 – 89	B+	67 – 69	D+
83 – 86	B	63 – 66	D
80 – 82	B-	60 – 62	D-
77 – 79	C+	Below 60	F

Grading Criteria
The following criteria are used for evaluating assignments. You can roughly translate a letter grade as the midpoint in the scale (for example, an A- equates to a 91.5).

Criteria	Grade
The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are no mechanical, grammatical, or organization issues that detract from the ideas.	A- or A
The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals.	B-, B, B+
The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions.	C-, C, C+
The assignment constantly fails to meet expectations. It is incomplete or in some other way consistently fails to demonstrate a firm grasp of the assigned material.	Below C-

Late Assignment Policy
An assignment is considered late if it is turned in after the assignment deadlines stated above. No late assignments will be accepted without penalty unless arrangements for validated unusual or unforeseen situations have been made.
- Participation and case study contributions cannot be turned in late. If you miss contributing prior to the deadlines for class that week you will receive no credit for it.
- Assignments will be assessed **a 20% penalty** each day they are late. No credit is given for assignments turned in over five calendar days past the due date.
- You must submit all assignments, even if no credit is given. **If you skip an assignment, an additional 10 points will be subtracted from your final grade in the course.**
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

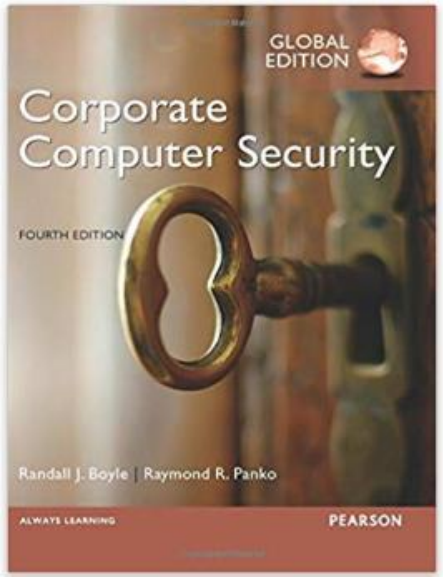


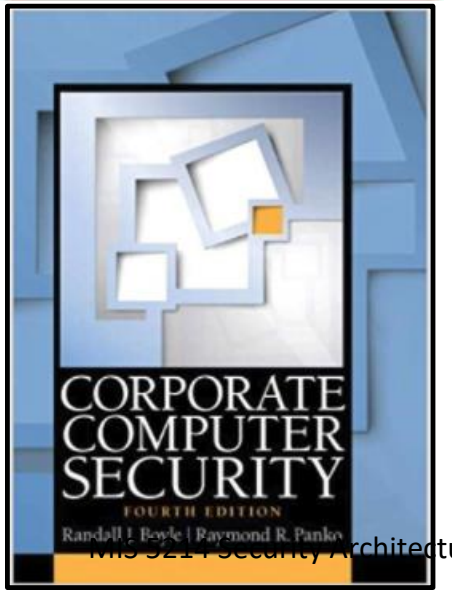
MIS5214 – Section 401 Syllabus Page 10

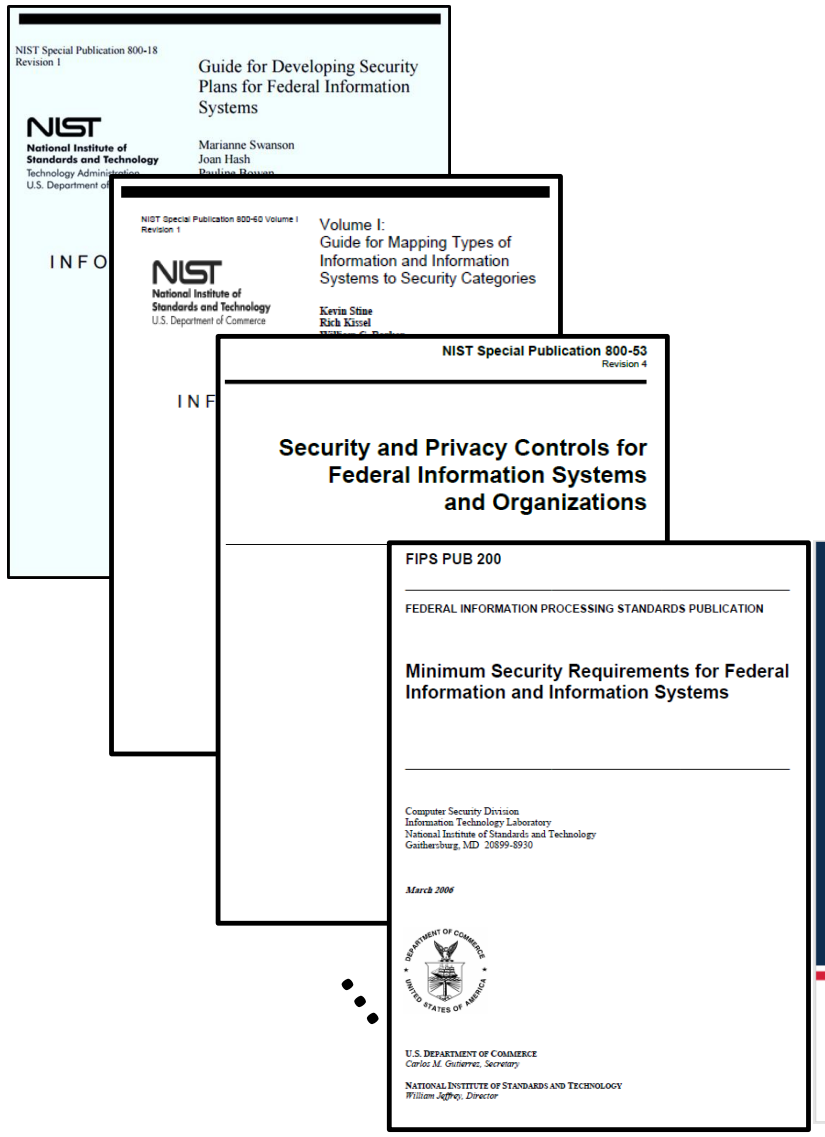
Additional Information

Availability of Instructor	• Please feel free to contact me via e-mail with any issues related to this class. I will also be available at the end of each session. Please note that these discussions are to address questions/concerns but are NOT for helping students catch up on content they missed because they were absent. Note: I will respond promptly when contacted during the week • I am available to meet personally with you: ✓ Immediately after class ✓ During office hours ✓ By appointment prior to class ✓ By appointment by phone
Attendance Policy	• Class discussion is intended to be an integral part of the course. Therefore, full attendance is expected by every student. • If you are absent from class, speak with your classmates to catch up on what you have missed.
Class Etiquette	• Please be respectful of the class environment. • Class starts promptly at the start time. Arrive on time and stay until the end of class. • Turn off and put away cell phones, pagers and alarms during class. • Limit the use of electronic devices (e.g., laptop, tablet computer) to class-related usage such as taking notes. Restrict the use of an Internet connection (e.g., checking email, Internet browsing, sending instant messages) to before class, during class breaks, or after class. • Refrain from personal discussions during class. Please leave the room if you need to speak to another student for more than a few words. If a student cannot refrain from engaging in private conversation and this becomes a pattern, the students will be asked to leave the classroom to allow the remainder of the students to work. • During class time speak to the entire class (or breakout group) and let each person "take their turn." • Be fully present and remain present for the entirety of each class meeting.

Textbook and Readings

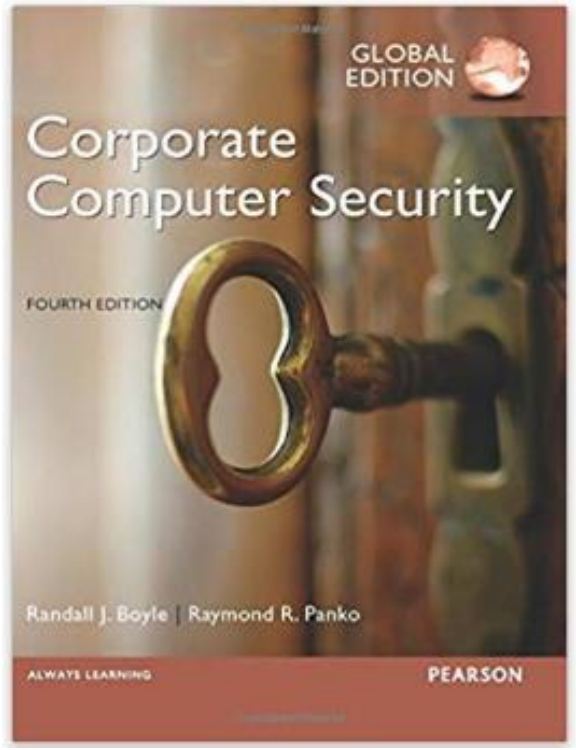




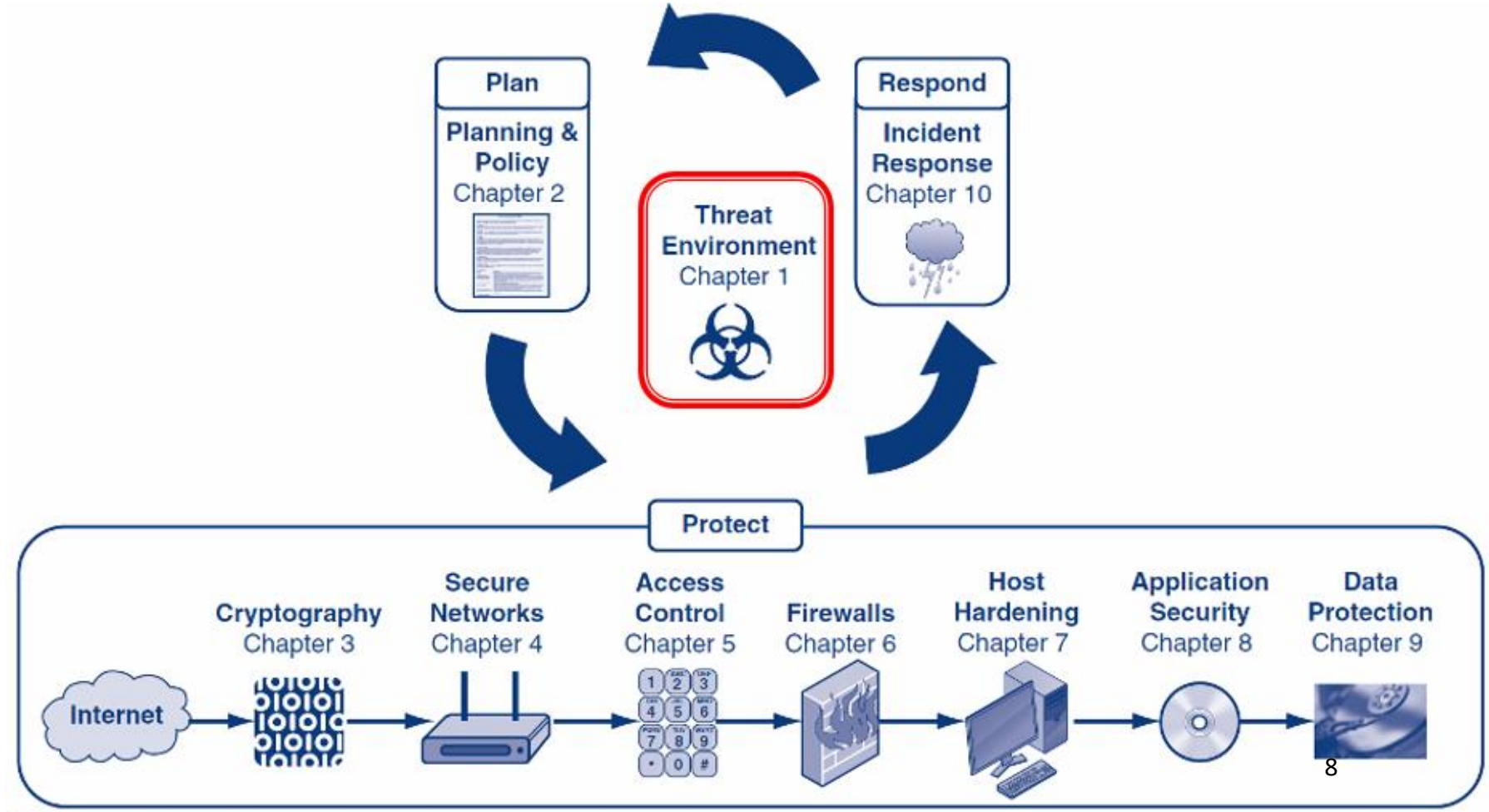


Unit #	Readings
1	• Boyle and Panko: Chapter 1 The Threat Environment • Ross, J.W., Weill P., and Robertson D.C. (2008), "Implement the Operating Model Via Enterprise Architecture" (in the Harvard Business Publishing course pack)
2	• NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 10 Risk Management, pp.84-95 • NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems" • "FedRAMP System Security Plan (SSP) High Baseline Template"
3	• Boyle and Panko, Chapter 2 Planning and Policy • NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 8 – Security Planning, pp.67-77 • NIST SP800-60V1R1 "Guide for Mapping Types of Information and Information Systems to Security Categories", pp.1-34 • FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems", pp.1-9
4	• Boyle and Panko, Chapter 3 Cryptography • NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations", pp.1-44 • NIST SP 800-53Ar4 " Assessing Security and Privacy Controls for Federal Information and Information Systems", pp.1-28
5	• Boyle and Panko, Module A "Networking Concepts" and Chapter 4 "Secure Networks" • NIST SP 800-145 "The NIST Definition of Cloud Computing" • An Introduction to DDoS – Distributed Denial of Service Attack • Public Key Infrastructure and X.509 Public Key Certificates
6	• Boyle and Panko: Chapter 6 Firewalls • Basile, C., Matteo, M.C., Mutti, S. and Paraboschi, S. "Detection of Conflicts in Security Policies", in Vacca, J.R. (2017) Computer and Information Security Handbook, Third Edition, Chapter 55. pp. 781-799.
8	• Boyle and Panko, Chapter 5 Access Control • NIST SP 800 63-3 "Digital Identity Guidelines" • NIST SP 800 63A "Digital Identity Guidelines Enrollment and Identity Proofing" • NIST SP 800 63B "Digital Identity Guidelines Authentication and Lifecycle Management"
9	• Boyle and Panko, Chapter 7 Host Hardening • NIST SP 800-123 Guide to General Sever Security
10	• Boyle and Panko, Chapter 8 Application Security • OWASP Top 10 • OWASP Attack Surface Cheat Sheet
11	• Boyle and Panko, Chapter 9 Data Protection
12	• Boyle and Panko, Chapter 10 Incident & Disaster Response • NIST SP 800 34r1 Contingency Planning Guide for Federal Information Systems

Organization of textbook

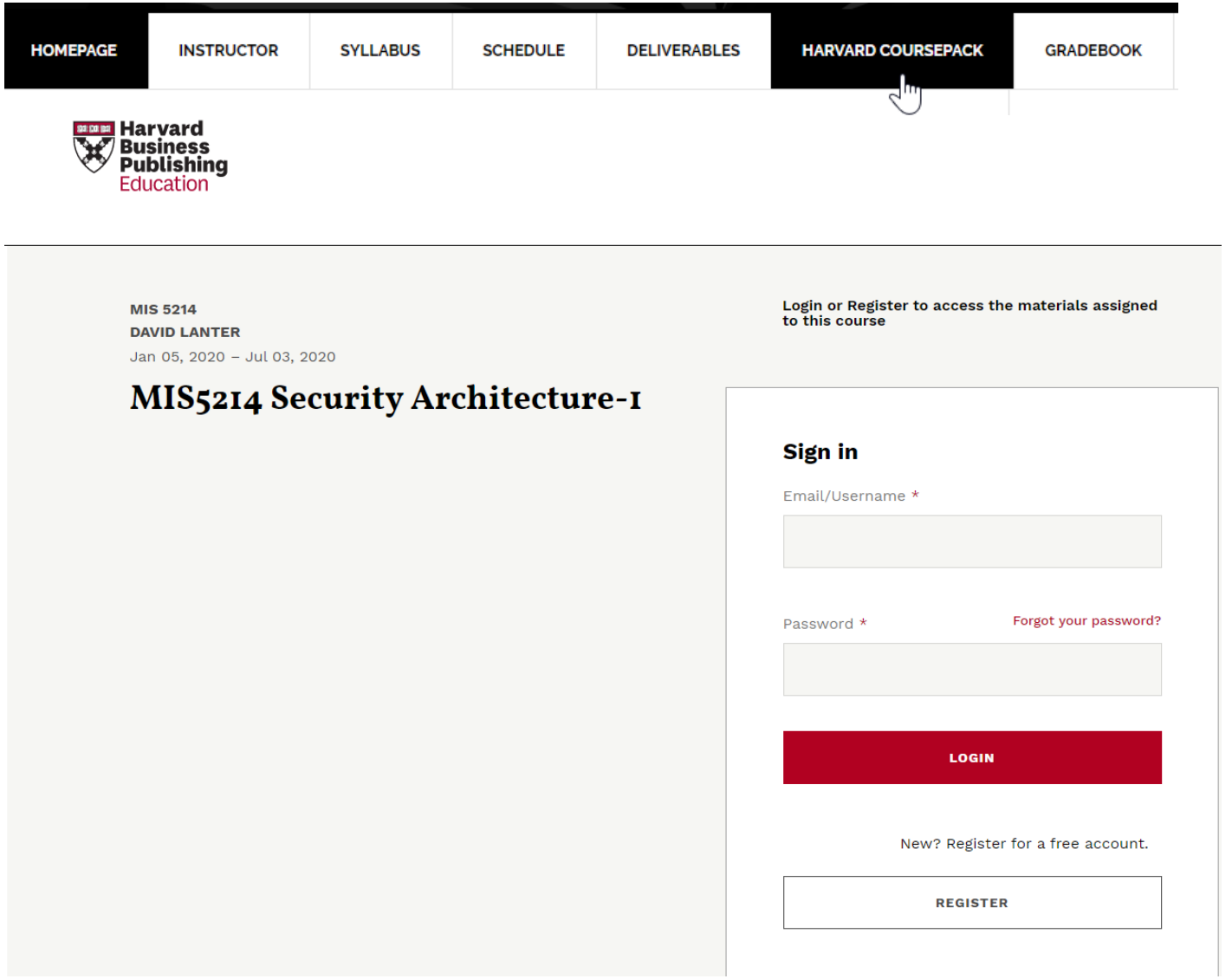


How is this book organized?



Harvard Business Publishing Course Pack

- 1 Reading
- 2 Case Studies



Class Schedule

Unit #	Topics	Date
1	Introduction	1/15
	The Threat Environment	
2	System Security Plan	1/22
3	Planning and Policy	1/29
4	Case Study 1 "*A High-Performance Computing Cluster Under Attack: The Titan Incident*"	2/5
	Cryptography	
5	Secure Networks	2/12
6	Firewalls, Intrusion Detection and Protection Systems	2/19
7	**Mid-Term Exam**	2/26
	Spring Break	3/4
8	Case Study 2 "Cyberattack: The Maersk Global Supply-Chain Meltdown"	3/11
	Access Control	
9	Host Hardening	3/18
10	Application Security	3/25
11	Data Protection	4/1
12	Incident and Disaster Response	4/8
13	Team Project Presentations	4/15
14	Team Project Presentations	4/22
15	**Final Exam**	

Readings listed under SCHEDULE

Unit 02 – System Security Plan

Readings

- NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 10 Risk Management, pp.84-95
- NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems"
- "FedRAMP System Security Plan (SSP) High Baseline Template"

Grading

Item	Weight
Assignments	20%
Participation (in class and online)	20%
Case Studies	20%
Team Project	20%
Exams	20%
	100%

Grading - Assignments

1. One Key Point Taken from Each Assigned Reading

   *Post one or two sentences of thoughtful analysis about one key point you took from each assigned reading by **midnight Sunday** the week they are due*

2. One Question You Would Ask Your Fellow Students to Facilitate Discussion
3. Problem Solving Assignments

Grading - Participation

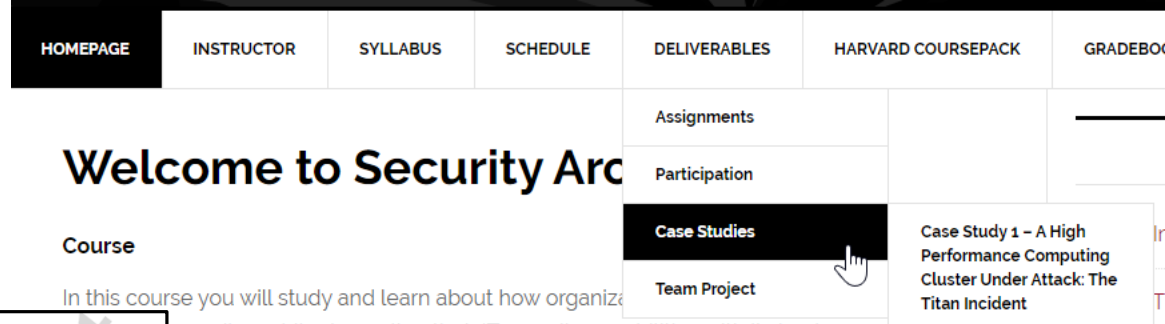
1. Comment on your classmates' discussion questions and/or key points they wrote about taking away from the readings

   Contribute at least three (3) substantive posts that include your thoughtful answers to their discussion questions and/or comments on the key points made by your classmates about the readings. Your posting of your three comments is due ***Tuesday by noon.***

2. Post an "In the News" article (link and brief summary)

   Be prepared to discuss in class an article you found about a current event in the Information Security arena. An ideal article would be tied thematically to the topic of the week. However, any article you find interesting and would like to share is welcome. The deadline for posting is ***Tuesday by noon.***

Grading - Case Studies



Journal of Information Technology Teaching Cases (2015) 5, 1–7
© 2015 JITTC Palgrave Macmillan All rights reserved 2043-8869/15
palgrave-journals.com/jittc/

JITT071

Teaching Case

A high performance computing cluster under attack: the Titan incident

Mark-David J McLaughlin[1,2], W Alec Cram[1], Janis L Gogan[1]

[1]Bentley University, Waltham, USA;
[2]Cisco Systems, San Jose, USA

Correspondence:
MDJ McLaughlin, Bentley University, 175 Forest St, Smith Technology Center, Waltham, MA 02452, USA.
Tel: +978 936 0188;
Fax: +781 891 2949

Abstract

At the University of Oslo (UiO), CERT manager Margrete Raaum learned of a network attack on Titan, a high-performance computing cluster that supported research conducted by scientists at CERT and other research institutions across Europe. The case describes the incident response, investigation, and clarification of the information security events that took place. As soon as Raaum learned of the attack, she ordered that the system be disconnected from the Internet to contain the damage. Next, she launched an investigation, which over a few days pieced together logs from previous weeks to identify suspicious activity and locate the attack vector. Raaum hopes to soon return Titan to its prior safe condition. In order to do so, she must decide what tasks still need to be completed to validate the systems and determine if it is safe to reconnect it to the Internet. She must also consider further steps to improve her team's ability to prevent, detect, and respond to similar incidents in the future. This case is designed for an undergraduate or graduate information security (infosec) class that includes students with varied technical and business backgrounds. The case supports discussion of technical and managerial infosec issues in inter-organizational systems – a topic that is currently underrepresented in major case collections.

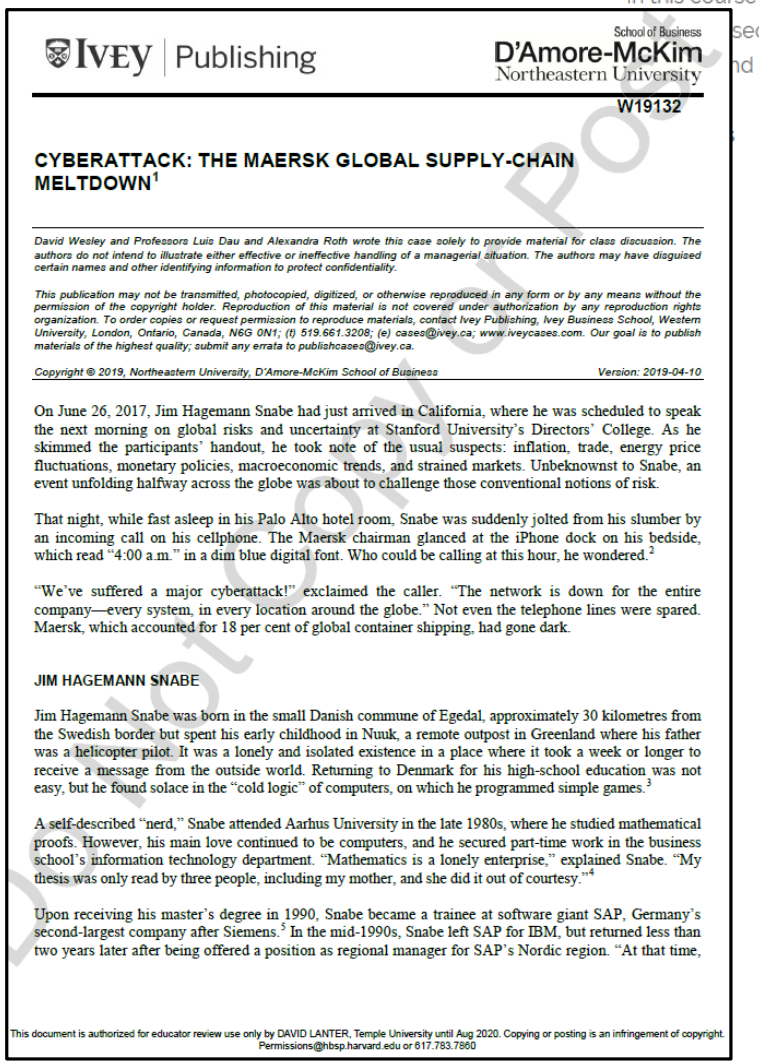
Journal of Information Technology Teaching Cases (2015) **5**, 1–7. doi:10.1057/jittc.2015.1;
published online 17 March 2015
Keywords: information security; incident response; risk management; inter-organizational collaboration; IT governance; high performance computing

Introduction

On the morning of 12 August, Margrete Raaum, Computing Emergency Response Team (CERT) manager at the University of Oslo (Universitetet i Oslo, UiO), sat down to drink a cup of strong coffee and reflect on the events of the previous two and a half days. Around 5 o'clock in the evening on 9 August, Raaum had returned to Norway after attending the annual DefCon security conference in Las Vegas[1] with several colleagues. She was drowsy from jet-lag when her phone had rung and an engineer in UiO's research computing operations group told her, "Um, I think there might have been a break-in on the Titan cluster."

Raaum now thought, "That may have been the understatement of the year," as she took another sip of coffee. UiO was a member of the Nordic DataGrid Facility (NDGF) of the European Grid Infrastructure (EGI). Titan, a high-performance computing cluster, was a shared resource that supported astrophysics research and other scientific initiatives sponsored by NDGF and/or EGI. The computational power supplied by Titan was essential to molecular biology research, DNA sequencing analysis, and petroleum reservoir simulations. Many scientists took advantage of Titan's extensive computational power by writing their own custom applications for their research. Ensuring the security of the Titan cluster was one of Raaum's many responsibilities, and she was well aware of a troubling worldwide trend: cybercriminals frequently broke into various organizations' networks to steal username and password combinations (credentials) and then (capitalizing on the knowledge that many users re-used their passwords on other sites) used the stolen credentials to attack higher value targets. So, instead of catching up on her sleep the evening of 9 August, Margrete Raaum was jolted into command mode.

News of the attack had triggered a maelstrom of international activity as Raaum and her team tried to determine what happened, contain the damage, and plan an orderly return to full operation. At Raaum's direction, the Titan master node



IVEY | Publishing

School of Business
D'Amore-McKim
Northeastern University

W19132

CYBERATTACK: THE MAERSK GLOBAL SUPPLY-CHAIN MELTDOWN[1]

David Wesley and Professors Luis Dau and Alexandra Roth wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

On June 26, 2017, Jim Hagemann Snabe had just arrived in California, where he was scheduled to speak the next morning on global risks and uncertainty at Stanford University's Directors' College. As he skimmed the participants' handout, he took note of the usual suspects: inflation, trade, energy price fluctuations, monetary policies, macroeconomic trends, and strained markets. Unbeknownst to Snabe, an event unfolding halfway across the globe was about to challenge those conventional notions of risk.

That night, while fast asleep in his Palo Alto hotel room, Snabe was suddenly jolted from his slumber by an incoming call on his cellphone. The Maersk chairman glanced at the iPhone dock on his bedside, which read "4:00 a.m." in a dim blue digital font. Who could be calling at this hour, he wondered.[2]

"We've suffered a major cyberattack!" exclaimed the caller. "The network is down for the entire company—every system, in every location around the globe." Not even the telephone lines were spared. Maersk, which accounted for 18 per cent of global container shipping, had gone dark.

JIM HAGEMANN SNABE

Jim Hagemann Snabe was born in the small Danish commune of Egedal, approximately 30 kilometres from the Swedish border but spent his early childhood in Nuuk, a remote outpost in Greenland where his father was a helicopter pilot. It was a lonely and isolated existence in a place where it took a week or longer to receive a message from the outside world. Returning to Denmark for his high-school education was not easy, but he found solace in the "cold logic" of computers, on which he programmed simple games.[3]

A self-described "nerd," Snabe attended Aarhus University in the late 1980s, where he studied mathematical proofs. However, his main love continued to be computers, and he secured part-time work in the business school's information technology department. "Mathematics is a lonely enterprise," explained Snabe. "My thesis was only read by three people, including my mother, and she did it out of courtesy."[4]

Upon receiving his master's degree in 1990, Snabe became a trainee at software giant SAP, Germany's second-largest company after Siemens.[5] In the mid-1990s, Snabe left SAP for IBM, but returned less than two years later after being offered a position as regional manager for SAP's Nordic region. "At that time,

Case study analysis

1. Individual preparation
2. Group discussion
3. Class discussion

Grading - Team Projects

By class 4, students will be organized into teams that work together on case studies and on the Team Project

Each team will be responsible for researching, developing and presenting a system security plan (SSP) for a cloud-based enterprise information system

SSP will include technical specifications and diagrams illustrating the logical network architecture and security architecture of an information system

Teams will develop and deliver a 15-minute presentation on the system's security architecture, followed by questioning by the other project teams

Unit #	Team Project Schedule	Due
8	1st Draft System Security Plan (SSP)	3/11
10	2nd Draft SSP	3/25
12	3rd Draft SSP	4/8
13	Presentation of Final Deliverables	4/15
14	Presentation of Final Deliverables	4/22

Grading - Exams

Unit #	Exam	Date
7	Mid-Term	2/26
	Final	4/29

Weekly Cycle

When	Actor	Task	Type
Thursday	Instructor	Post readings & assignment questions	Assignment
Sunday midnight	Student	Post key points, question, (& answers)	Assignment
Sunday midnight	Student	Case study answers	Assignment
Tuesday noon	Student	Post 3 comments and In The News article	Participation
Wednesday	Both of Us	Class meeting	Participation

Agenda

- ✓Welcome and Introductions
- ✓Course Introduction Goals
- Introductory Terminology
- The Threat Environment
- Next Week…

Introductory Terminology

"Information security" is protection of…

- Confidentiality, integrity, and availability ("CIA") of data and information
- Data, information and information systems from unauthorized…
  - Access, use, disclosure = **Confidentiality**
  - Modification = **Integrity**
  - Disruption or destruction = **Availability**

Terminology: Security Goals

Confidentiality

- Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network

Terminology: Security Goals

Integrity

- Integrity means that attackers cannot change or diminish information, either while it is on a computer or while it is traveling across a network
- …if information is changed or diminished, then the receiver can detect the change and possibly restore the data

Terminology: Security Goals

Availability

- People who are authorized to use information are not prevented from doing so

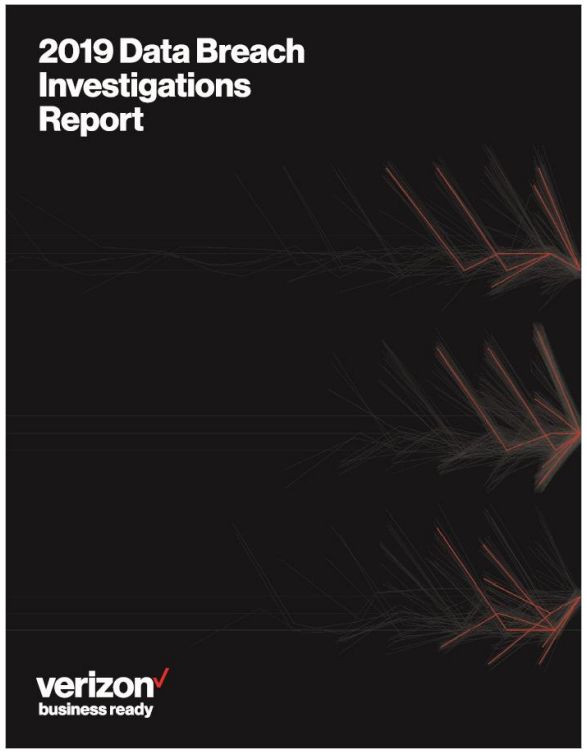
Terminology: Compromises

- Successful attacks
- Also called incidents
- Also called breaches (not breeches)

Terminology: Countermeasures

- Tools used to thwart attacks
- Also called safeguards, protections, and controls
- Types of countermeasures
  - Preventative
  - Detective
  - Corrective

Threat Environment



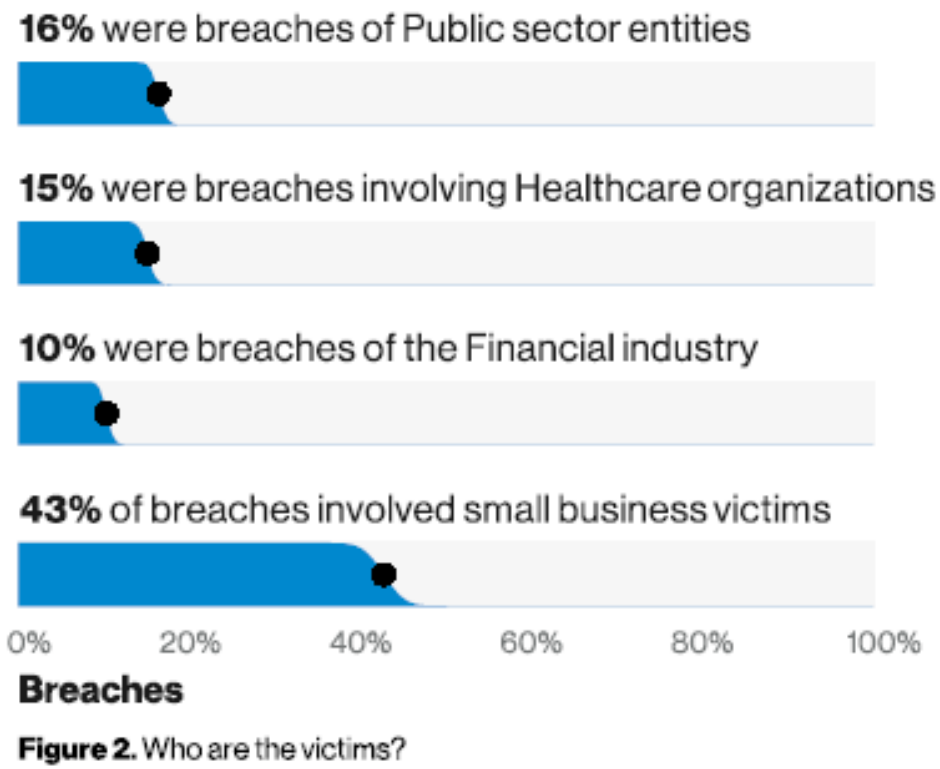


Figure 2. Who are the victims?

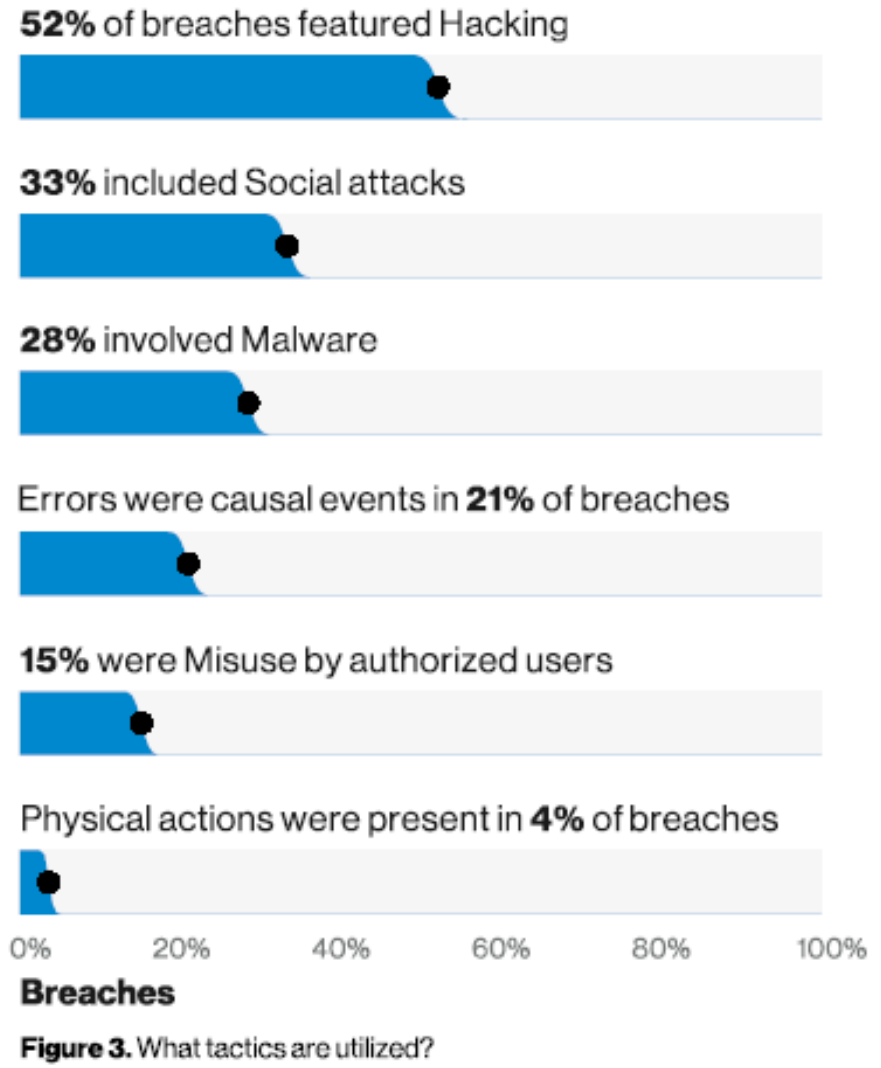
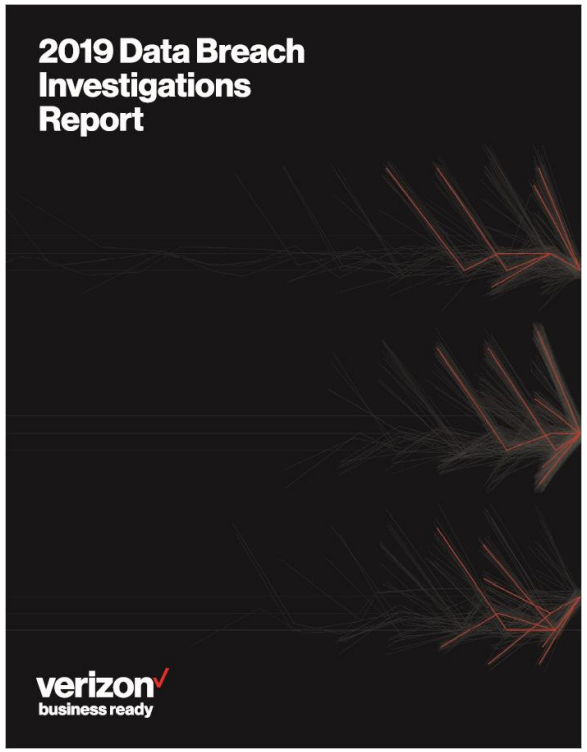


Figure 3. What tactics are utilized?

Based on "analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches."

Threat Environment



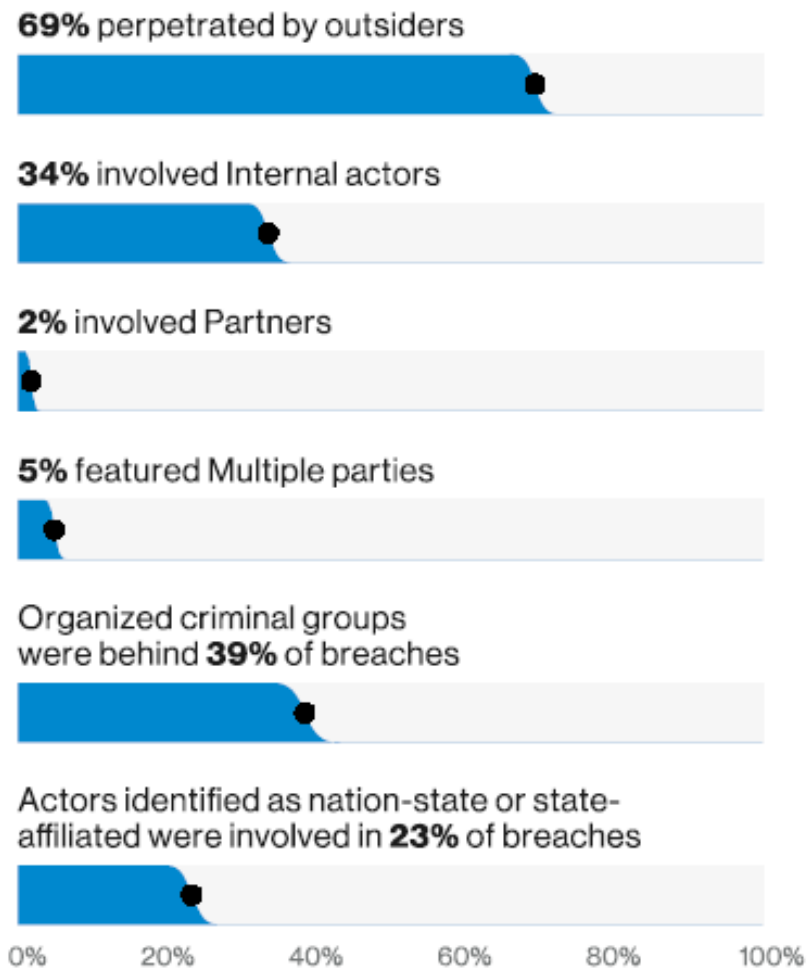


Figure 4. Who's behind the breaches?

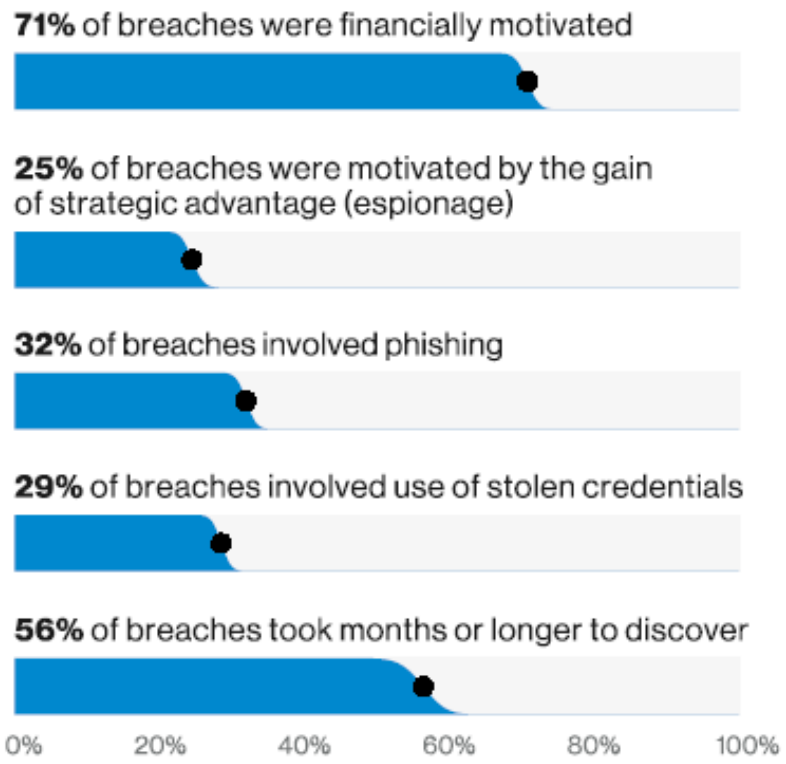
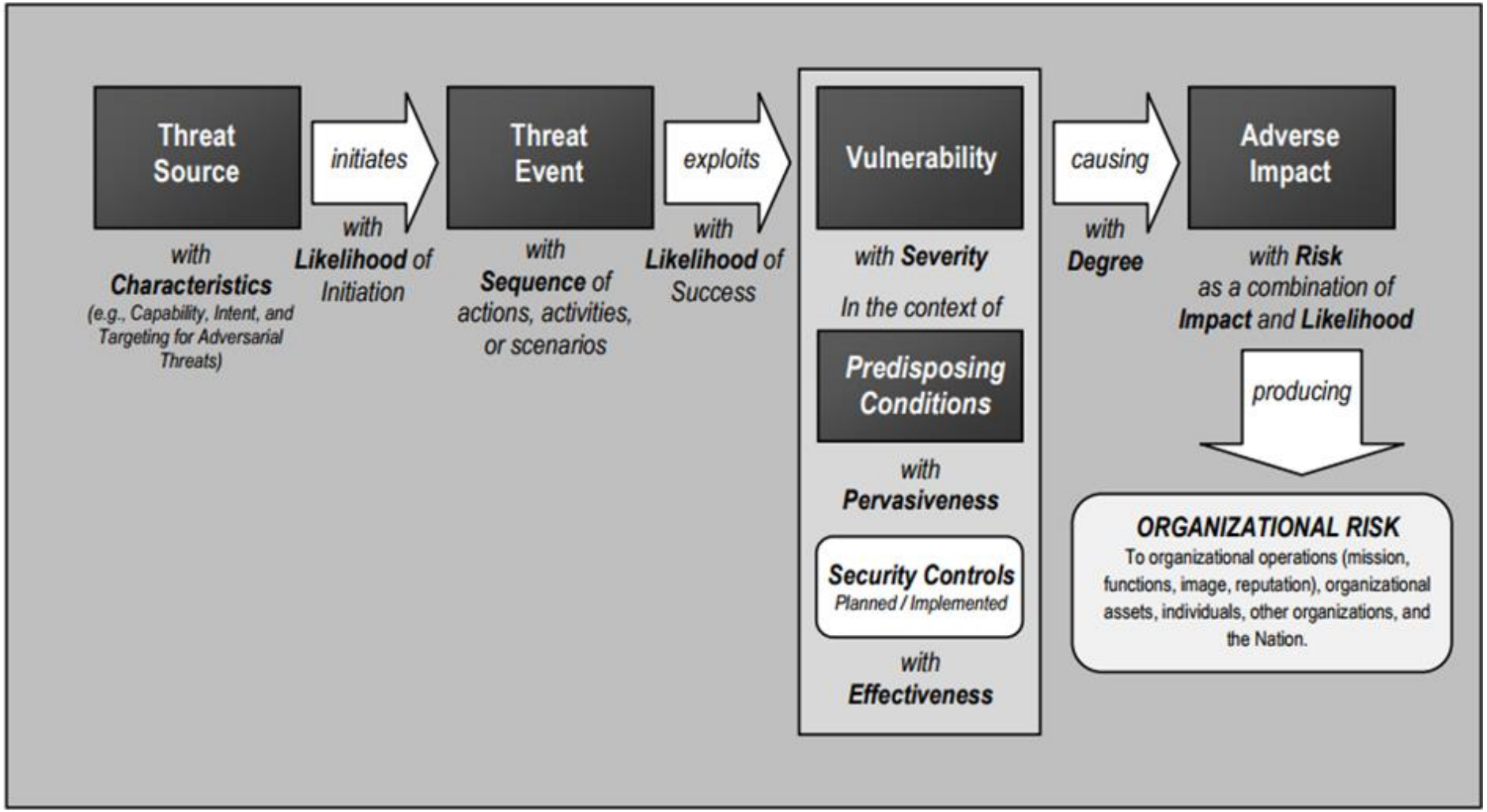


Figure 5. What are other commonalities?

Based on "analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches."

Security architects think about the interactions among threats, vulnerabilities, impacts and risks



From NIST 800-30r1 **Guide for Conducting Risk Assessment p. 12**

The Threat Environment

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

Adversarial (i.e. purposeful) threat sources

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 66

What type of Hacker are you?

"You need to decide if you're going to aspire to safeguarding the common good or settle for pettier goals. Do you want to be a mischievous, criminal hacker or a righteous, powerful defender?

…the best and most intelligent hackers work for the good side. They get to exercise their minds, grow intellectually, and not have to worry about being arrested. They get to work on the forefront of computer security, gain the admiration of their peers, further human advancement in the name of all that is good, and get well paid for it."

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Most Hackers Aren't Geniuses

"…readers often assume" bad-guy hackers are super smart, "…because they appear to be practicing some advanced black magic that the rest of the world does not know. In the collective psyche of the world, it's as if 'malicious hacker' and 'super-intelligence' have to go together.

A few are smart, most are average, and some aren't very bright at all, just like the rest of the world. Hackers simply know some facts and processes that other people don't, just like a carpenter, plumber, or electrician."

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Defenders are Hackers Plus

"If we do an intellectual comparison alone, the defenders on average are smarter than the attackers. A defender has to know everything a malicious hacker does plus how to stop the attack. And that defense won't work unless it has almost no end-user involvement, works silently behind the scenes, and works perfectly (or almost perfectly) all the time.

Show me a malicious hacker with a particular technique, and I'll show you more defenders that are smarter and better. It's just that the attacker usually gets more press." It's time for equal time for the defender!

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Hackers are Special

While not all are super-smart, “they all share a few common traits:”

- Broad intellectual curiosity
- Willingness to try things outside the given interface or boundary
- Not afraid to make their own way
- Usually they are life hackers:
  - Hacking all sorts of things beyond computers
  - Questioning the status quo and exploring all the time

- Most useful trait:
  - Persistence
  - Malicious hackers look for defensive weaknesses
  - Both malicious hackers and defenders are looking for weaknesses, just from opposite sides of the system
  - Both sides participate in an ongoing war with many battles, wins and losses. The most persistent side wins

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

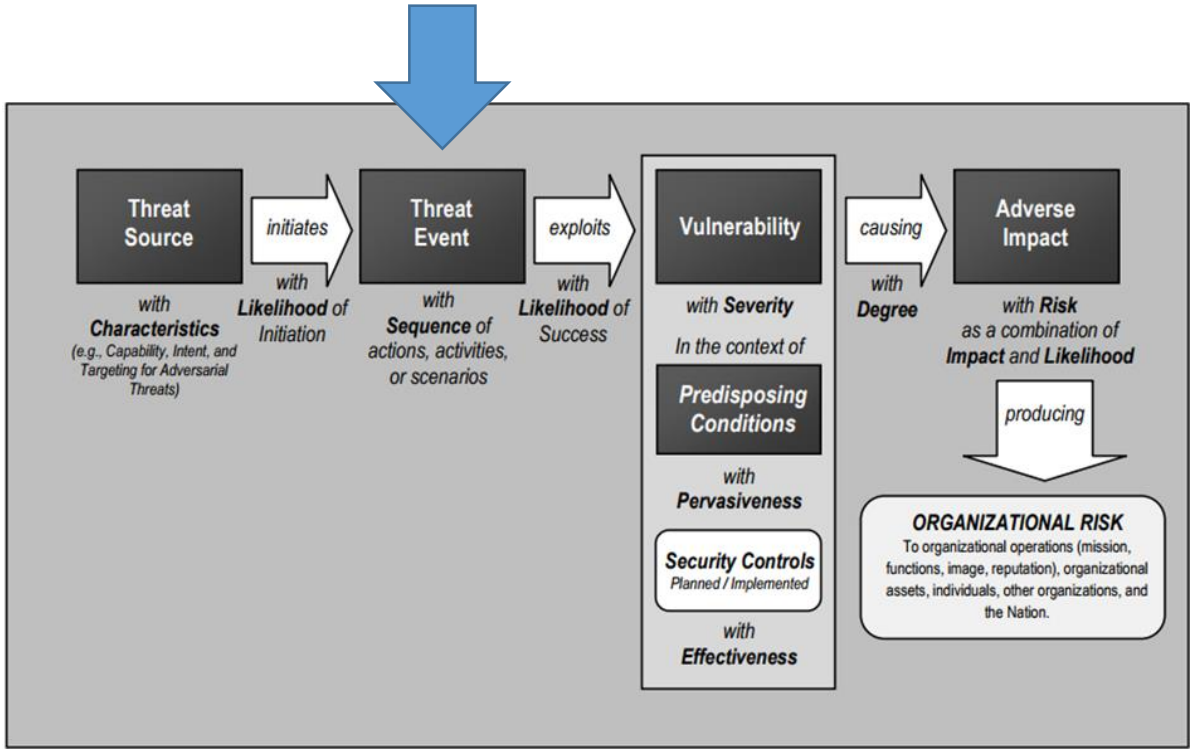
The Secret to Hacking

"If there is a secret to how hackers hack, it's that there is no secret to how they hack. It's a process of learning the right methods and using the right tools for the job…. There isn't even one way to do it. There is, however, a definitive set of steps that describe the larger, encompassing process"

Hacking Methodology Model

1. Information gathering ("reconnaissance")
2. Penetration
3. *Optional: Guaranteeing future easier access*
4. Internal reconnaissance
5. *Optional: Movement*
6. Intended action execution (e.g. data exfiltration)
7. *Optional: Covering Tracks*

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons



C2 = Command & Control malware

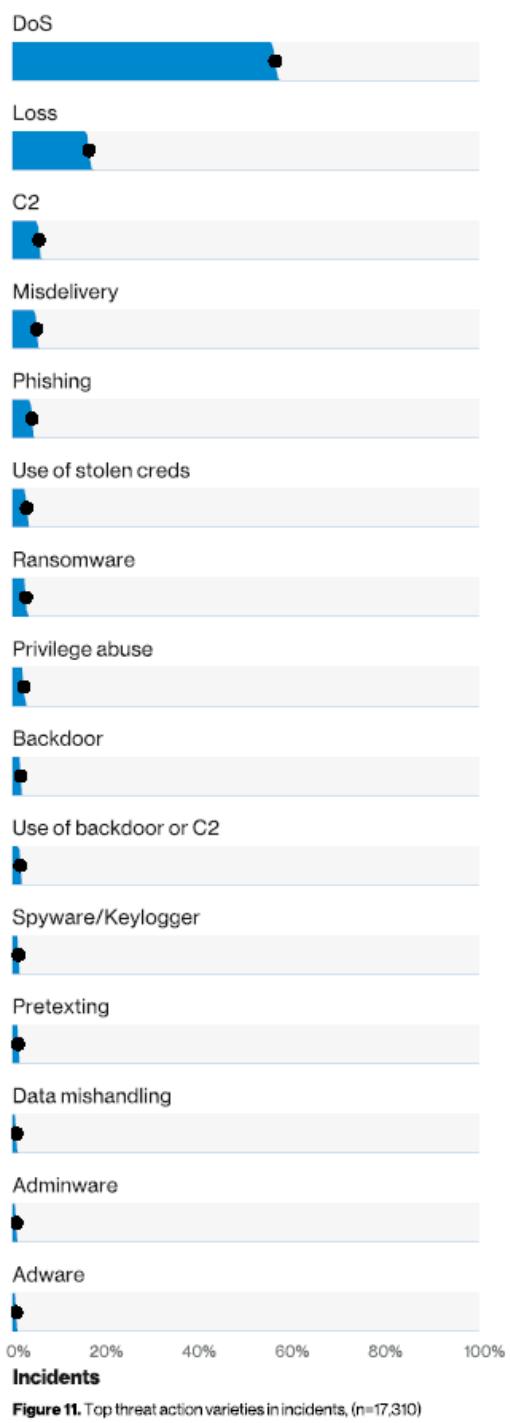


Figure 11. Top threat action varieties in incidents, (n=17,310)

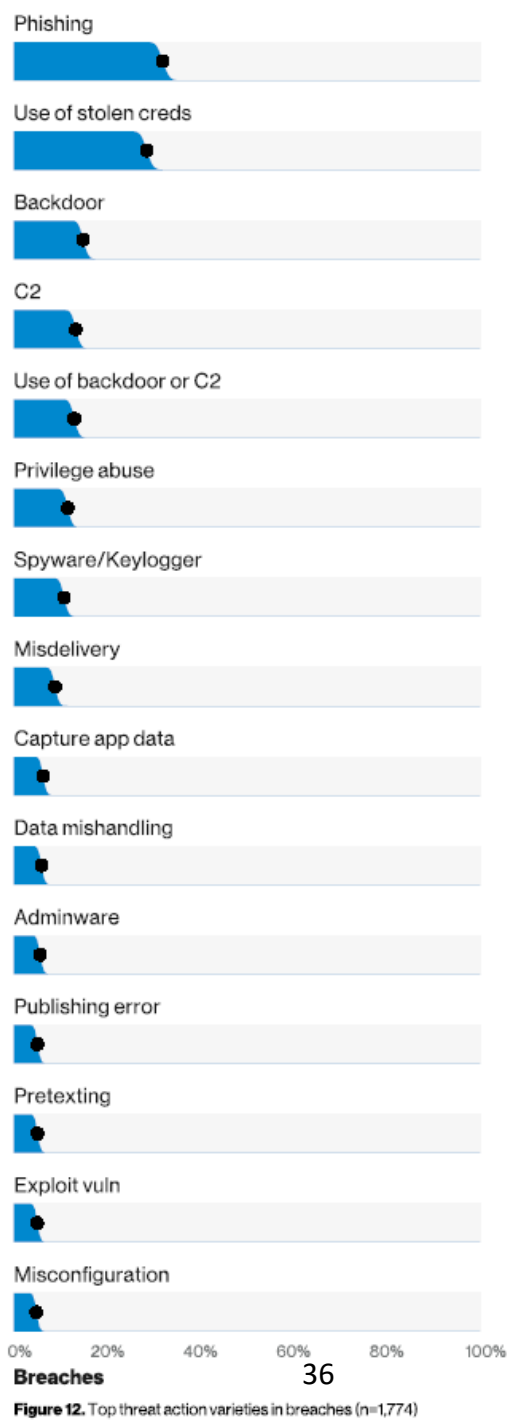
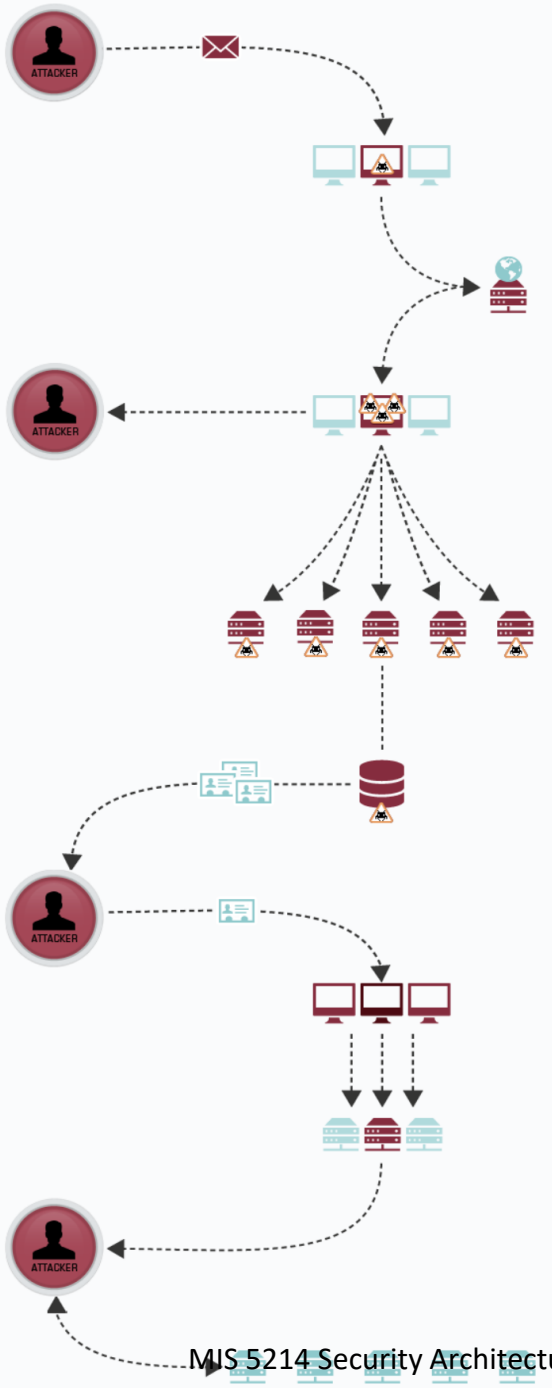


Figure 12. Top threat action varieties in breaches (n=1,774)

Anatomy of an Attack

(MANDIANT, 2015)



1. **Attacker sends spear phishing e-mail**
2. **Victim opens attachment**
   - Custom malware is installed
3. **Custom malware communicates to control web site**
   - Pulls down additional malware
4. **Attacker establishes multiple backdoors**

Threat landscape

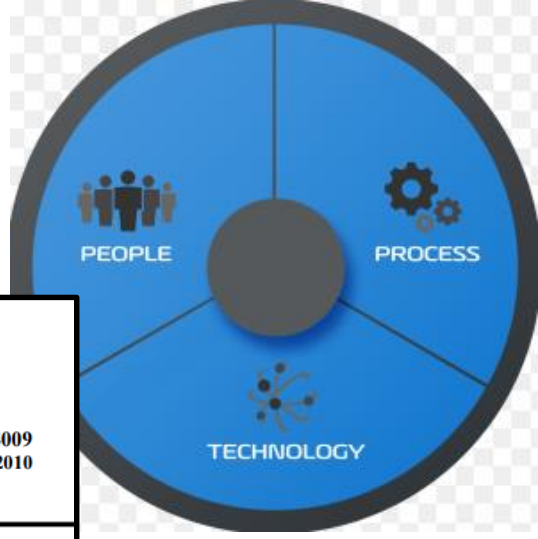
5. **Attacker accesses system**
   - Dumps account names and passwords from domain controller
6. **Attacker cracks passwords**
   - Has legitimate user accounts to continue attack undetected
7. **Attacker reconnaissance**
   - Identifies and gathers data
8. **Data collected on staging server**
9. **Data ex-filtrated**
10. **Attacker covers tracts**
    - Deletes files
    - Can return any time

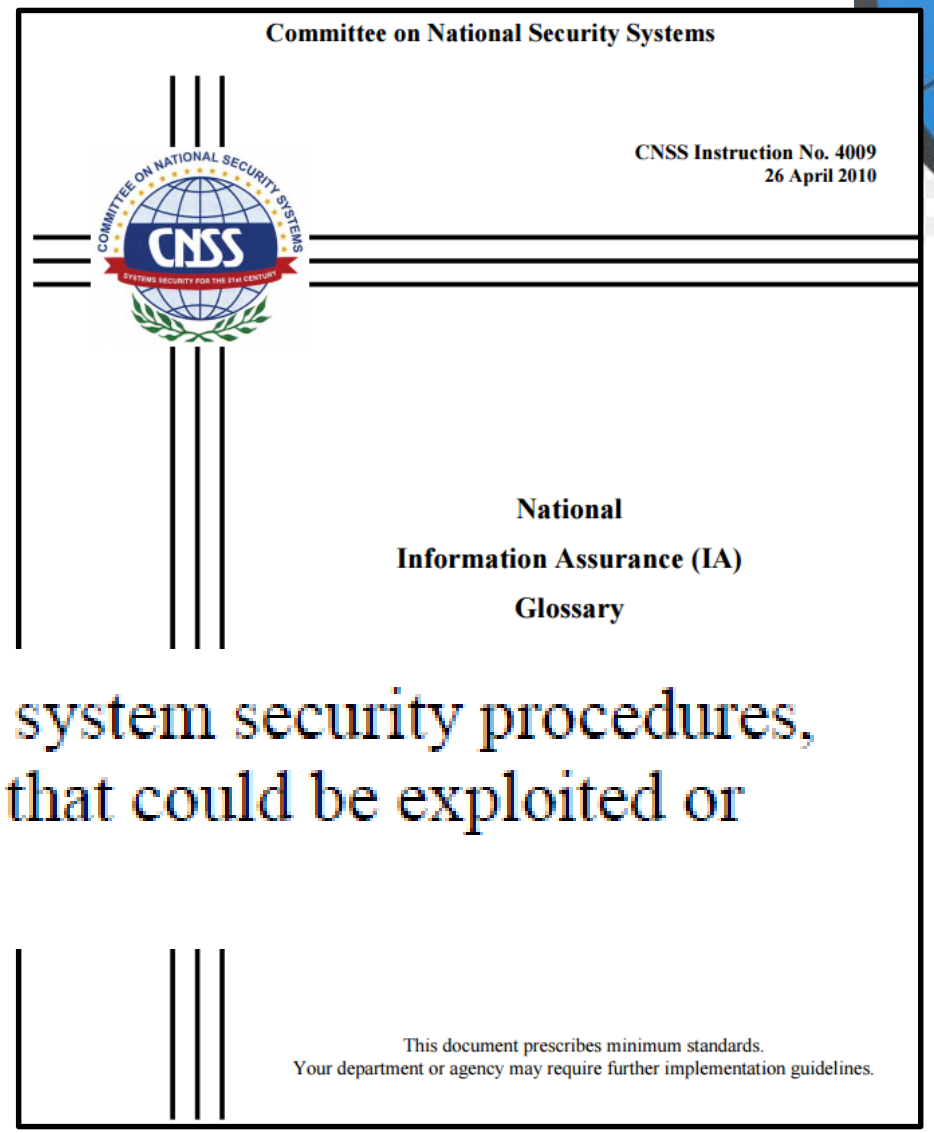
Advanced persistent threats (APT) *usually maintain remote access to target environments for 6-18 months before being detected (i.e. they are persistent)*

(Holcomb & Stapf, 2014)

What is a Vulnerability?

Any unaddressed susceptibility to a physical, technical or administrative information security threat




Committee on National Security Systems

CNSS Instruction No. 4009
26 April 2010

National
Information Assurance (IA)
Glossary

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

This document prescribes minimum standards.
Your department or agency may require further implementation guidelines.

Vulnerabilities can be classified by asset class

- Physical examples
  - Buildings in environmental hazard zones (e.g. low floor in flood zone)
  - Unlocked and unprotected doors to data center
  - Unreliable power sources
- Technical examples
  - Hardware – susceptibility to humidity, dust, soiling, unprotected storage
  - Software – insufficient testing, lack of audit trail, poor or missing user authentication and access control
  - Data – unencrypted transfer or storage, lack of backup
  - Network – Unprotected communication lines, insecure architecture
- Organizational examples
  - Inadequate screening and recruiting process, lack of security awareness and training
  - Lack of regular audits
  - Lack of security and IT related business continuity plans

http://www.infosightinc.com/collaterals/CVA-PT_March2016.pdf

What is a Risk?

A measure of threat

Potential loss resulting from unauthorized:

- *Access, use, disclosure*
- *Modification*
- *Disruption or destruction*

…of an enterprises' information

*Can be expresses in **quantitative** and **qualitative** terms*

Steps in a risk assessment methodology

1. What are the business assets ?
2. What possible threats put the business assets at risk ?
3. Which vulnerabilities and weaknesses may allow a threat to exploit the assets ?
4. For each threat, if it materialized, what would be the business impact on the assets ?

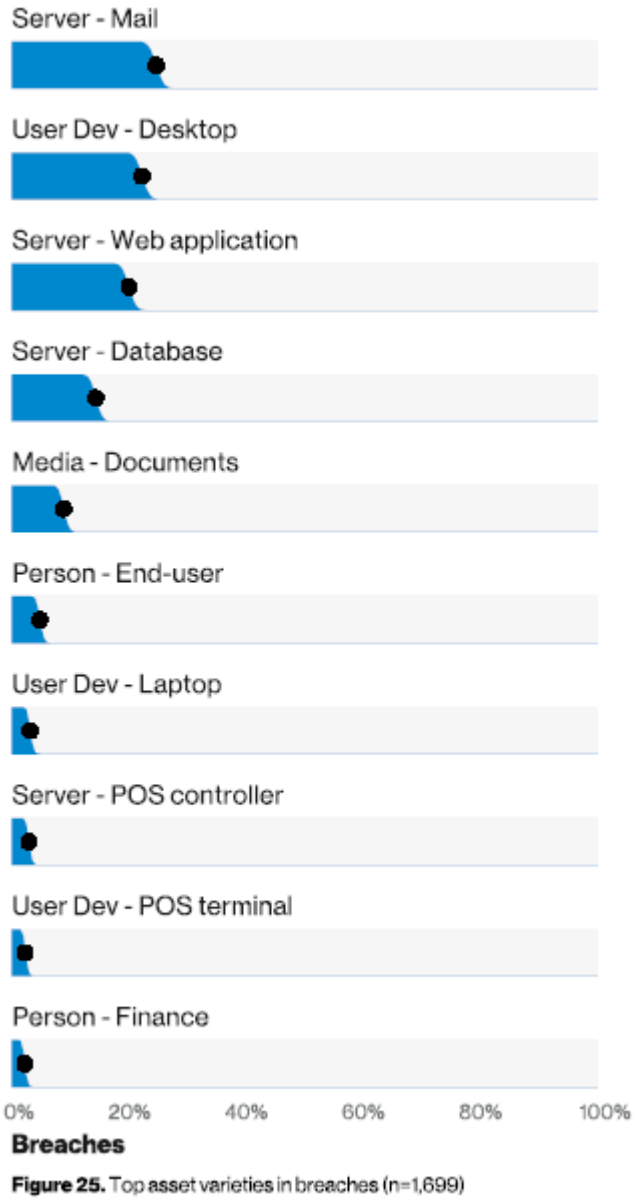


Figure 25. Top asset varieties in breaches (n=1,699)

Assessing risk – quantitative method

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

   – **Single loss expectancy (SLE) = Asset value X Exposure factor**

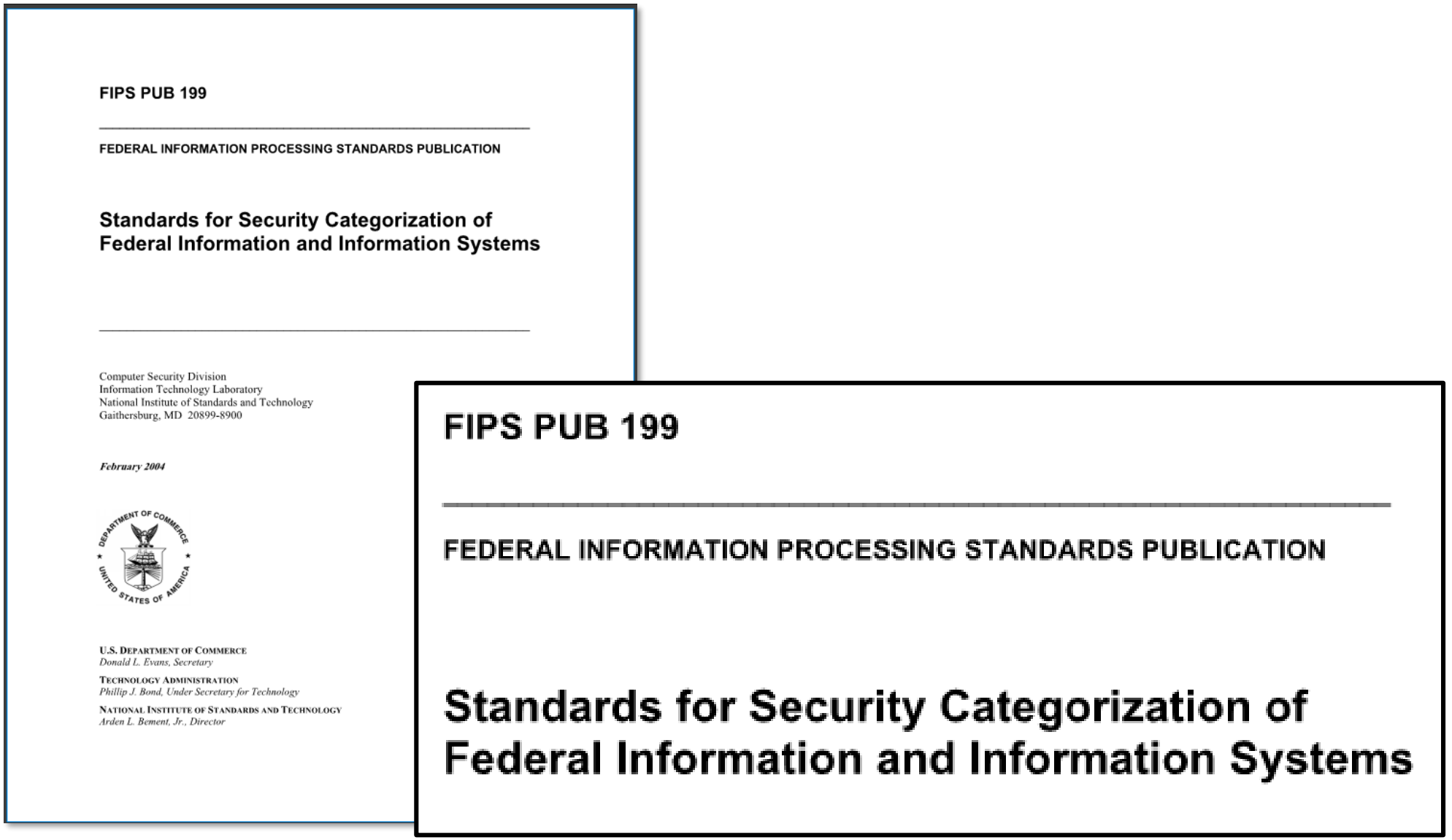
   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the **annual rate of occurrence (ARO)**. Simply stated, **how many times is this expected to happen in one year?**

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

   – **Annualized loss expectancy (ALE) = Single loss expectancy (SLE) X Annualized rate of occurrence (ARO)**

Assessing risk – qualitative method



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of
Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

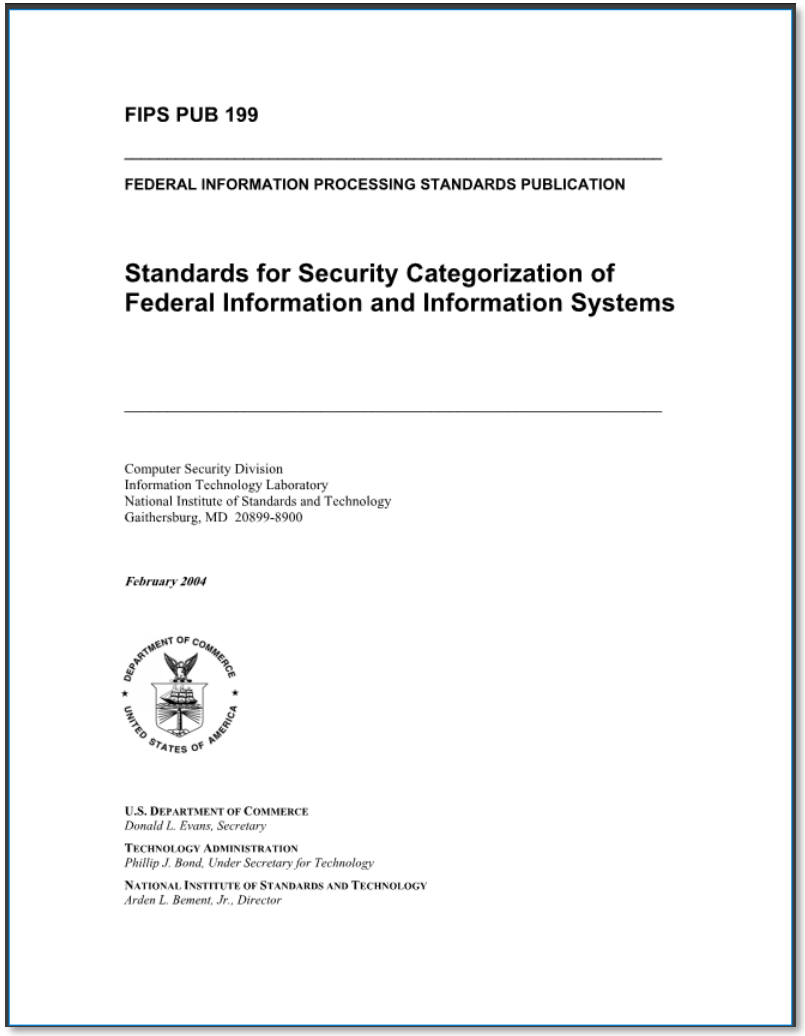
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of
Federal Information and Information Systems

FIPS 199: Risk assessment based on security objectives and impact ratings



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Architecture

A comprehensive and rigorous method to plan, design and describe current and desired future structure and behavior of an organization's:

- Business sub-units
- Processes and Personnel
- Information security systems

…so they align with the organization's core goals and strategic direction

Wikipedia: https://en.wikipedia.org/wiki/Enterprise_information_security_architecture

Security Architecture

"…the art and science of designing and supervising the construction of business systems, usually business information systems, which are:

- Free from danger, damage, etc.
- Free from fear, care, etc.
- In safe custody
- Not likely to fail
- Able to be relied upon
- Safe from attack"

Sherwood et al. (2005) Enterprise Security Architecture: A Business-Driven Approach

Defenders must be perfect

"One mistake by the defender essentially renders the whole defense worthless"

…every computer and software program must be patched, every configuration appropriately secure, and every end-user perfectly trained. Or at least that is the goal.

The defender knows that applied defenses may not always work or be applied as instructed, so they create "defense-in-depth" layers."

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

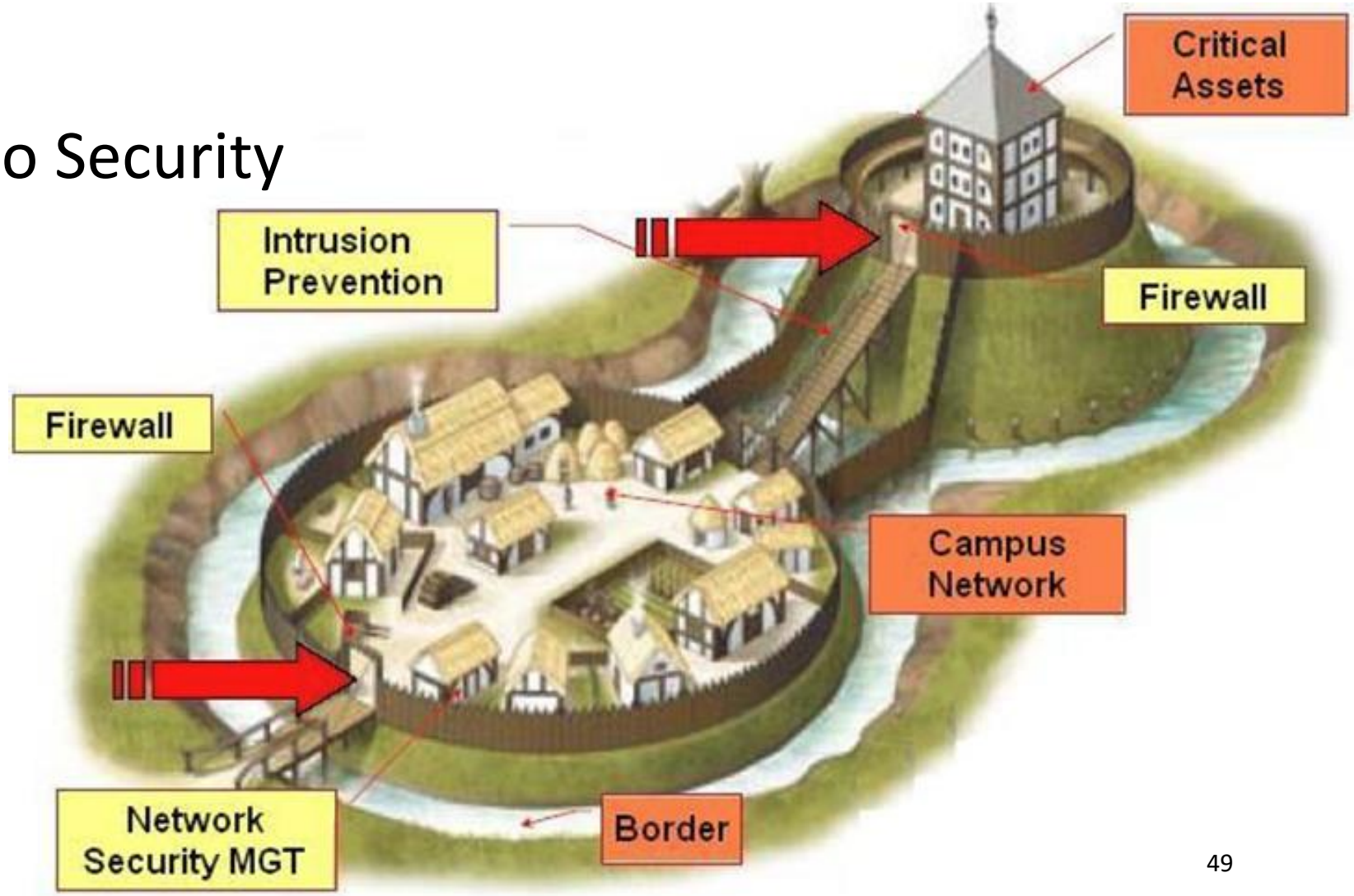
Security Architecture

Thinking about security architecture enables understanding enterprise information systems the way attackers do – as large diverse attack surfaces

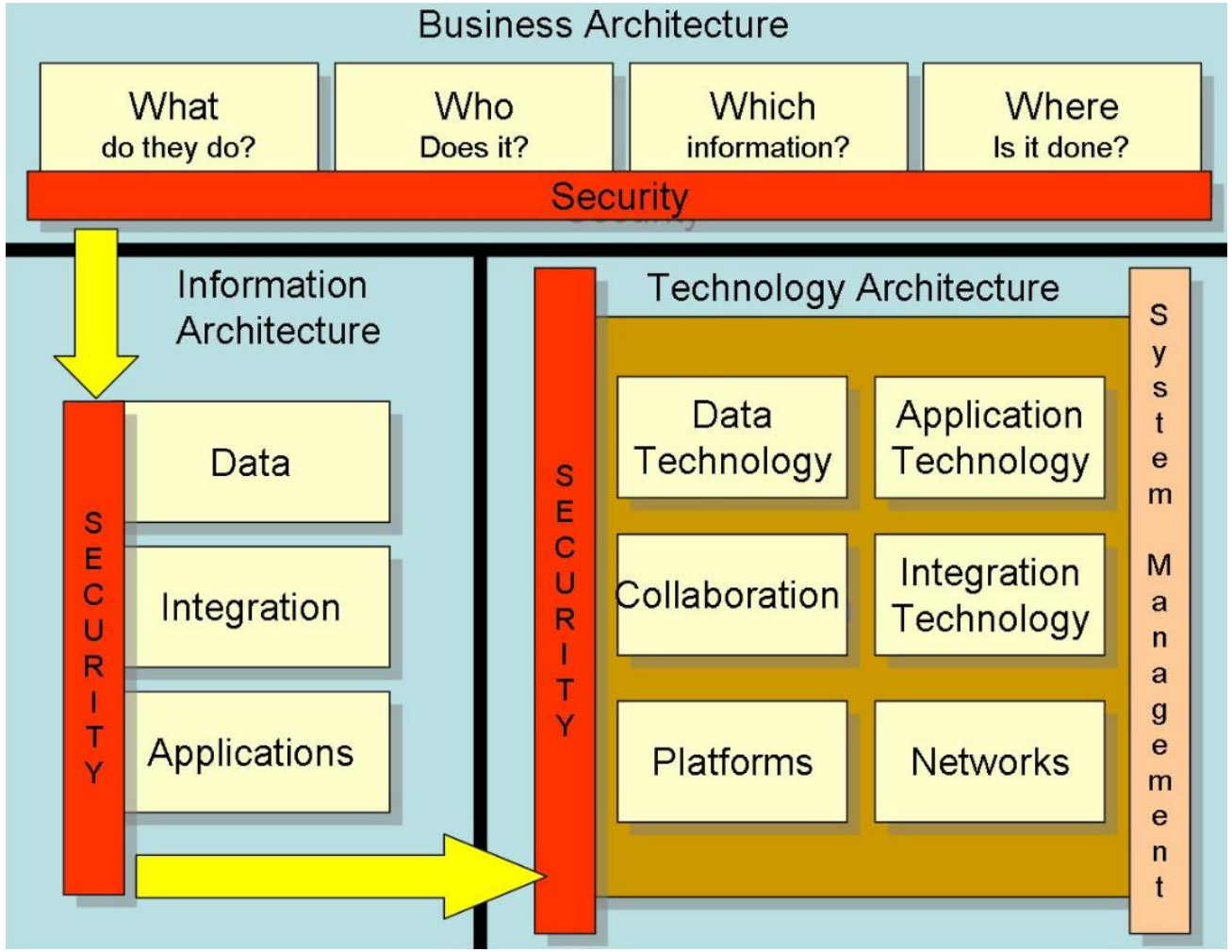
https://graquantum.com/blog/cyber-basics-cyber-attack-surface/

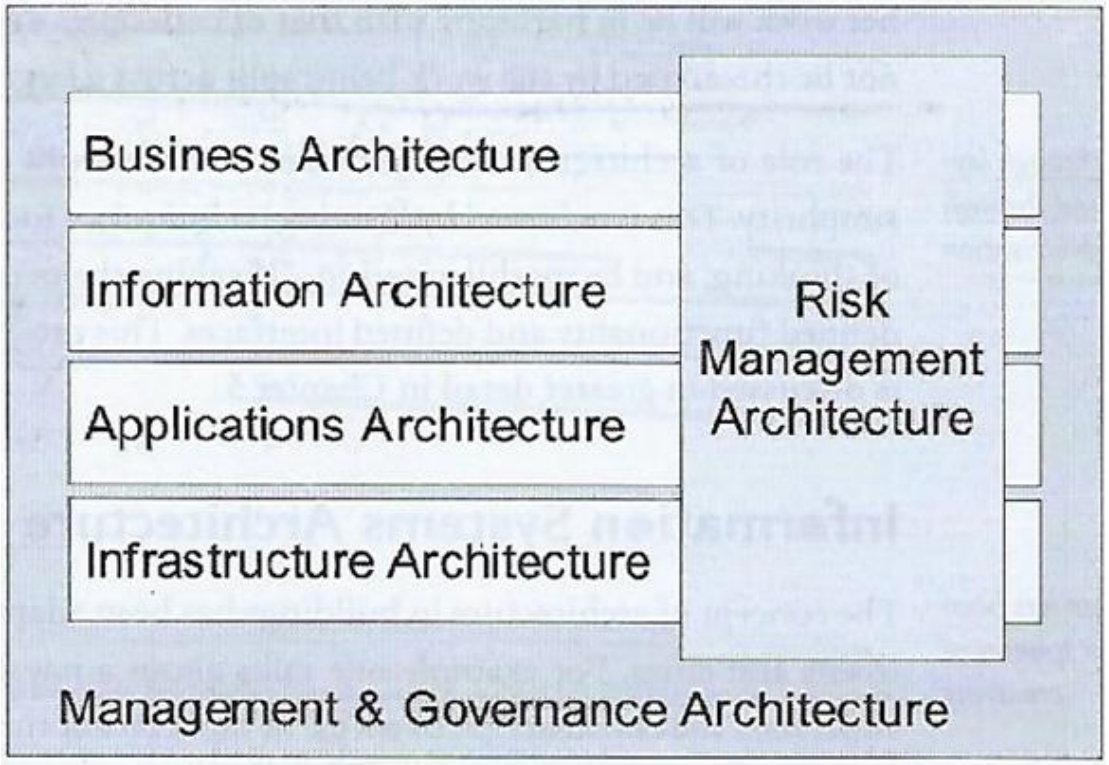
Defense in Depth

- Also known as:
  - Layered Security
  - Castle Approach to Security



Enterprise Information and Security Architecture





Sherwood et al. (2005) Enterprise Security Architecture: A Business-Driven Approach

Huxham, H. (2006) "Own view of Enterprise Information Security Architecture (EIS))Framework"
Wikipedia. https://en.wikipedia.org/wiki/Enterprise_information_security_architecture, accessed 2017-1-19

Security architecture questions

1. What is the system that is/has being/been built?
2. What can go wrong with it once it is built?
3. What should be done about those things that can go wrong?
4. Did you do a good job in your analysis?

Threat Modeling: Designing for Security, Adam Shostack, 2014

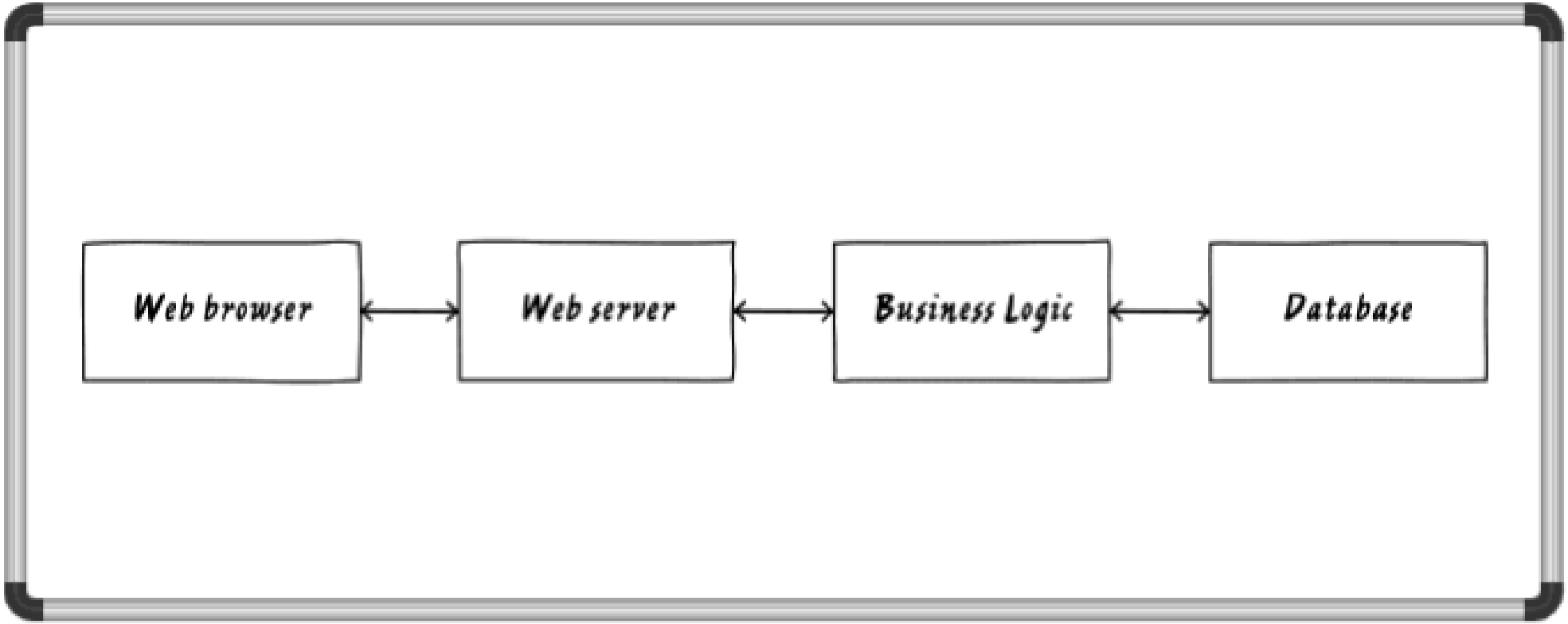
Security architecture framework

1. Model the system that is being built, deployed, or changed
2. Find threats using that model
3. Address (i.e. mitigate/control) the threats
4. Validate the mitigations for completeness and effectiveness

Threat Modeling: Designing for Security, Adam Shostack, 2014

What is the system that is/has being/been built?

- Draw a picture…
- What can go wrong here?

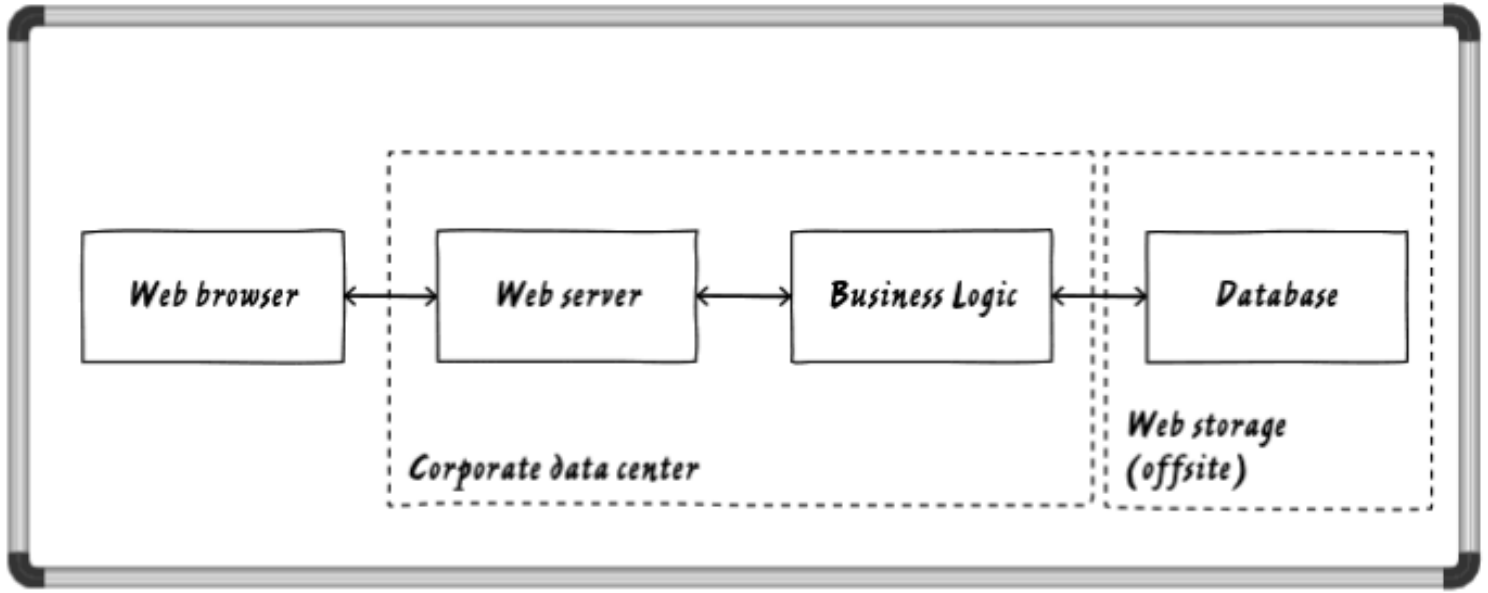


Threat Modeling: Designing for Security, Adam Shostack, 2014

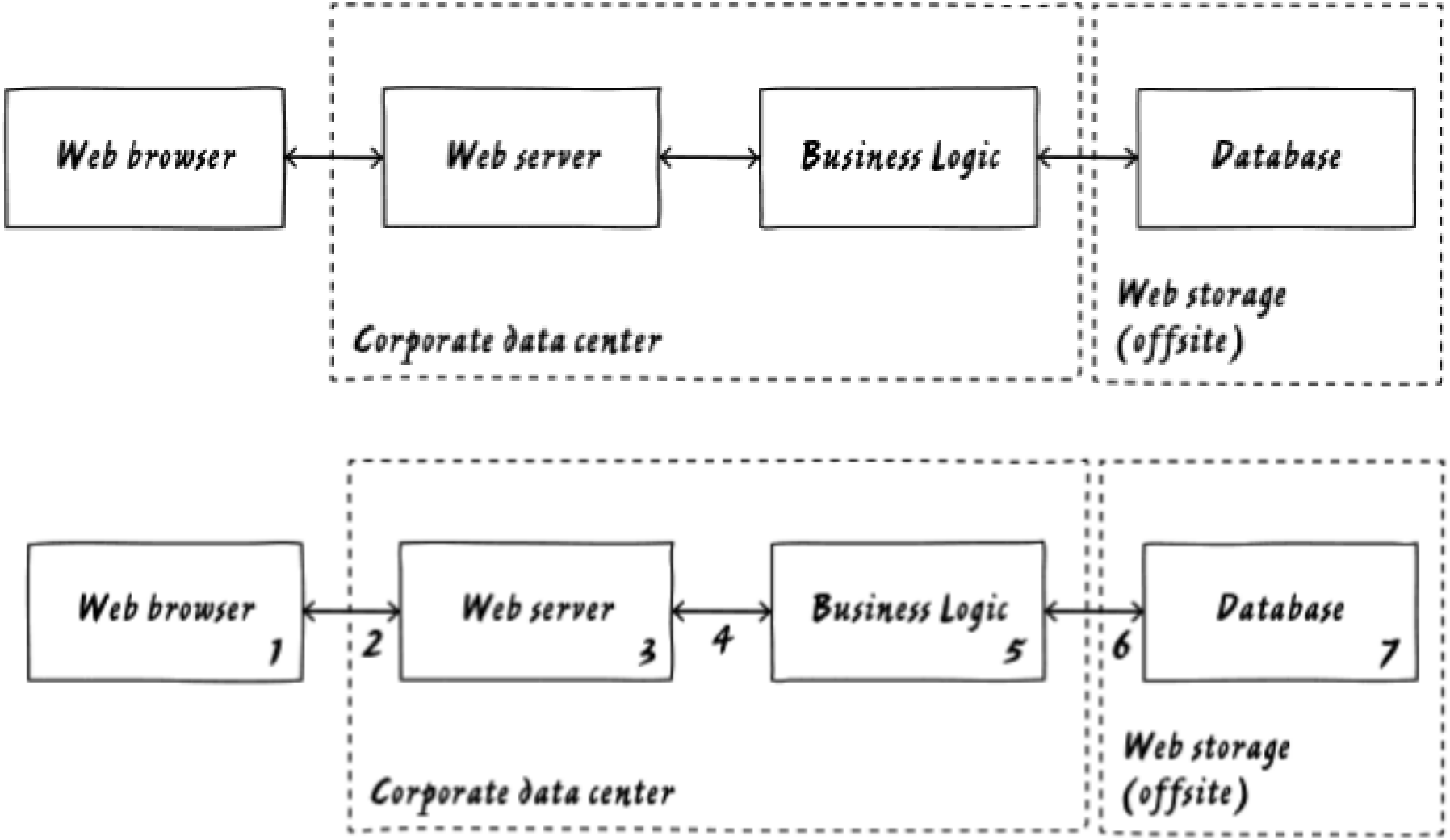
Draw and identify trust boundaries ("attack surfaces") in the system diagram

…these are found wherever different people can access and control different parts of the system

- Organizational boundaries
- Different physical computers or virtual machines
- Different subsystems
- Different access points or network interfaces
- Almost anywhere there will/should be different privileges



What can go wrong?
Where are the attack surfaces in this system?

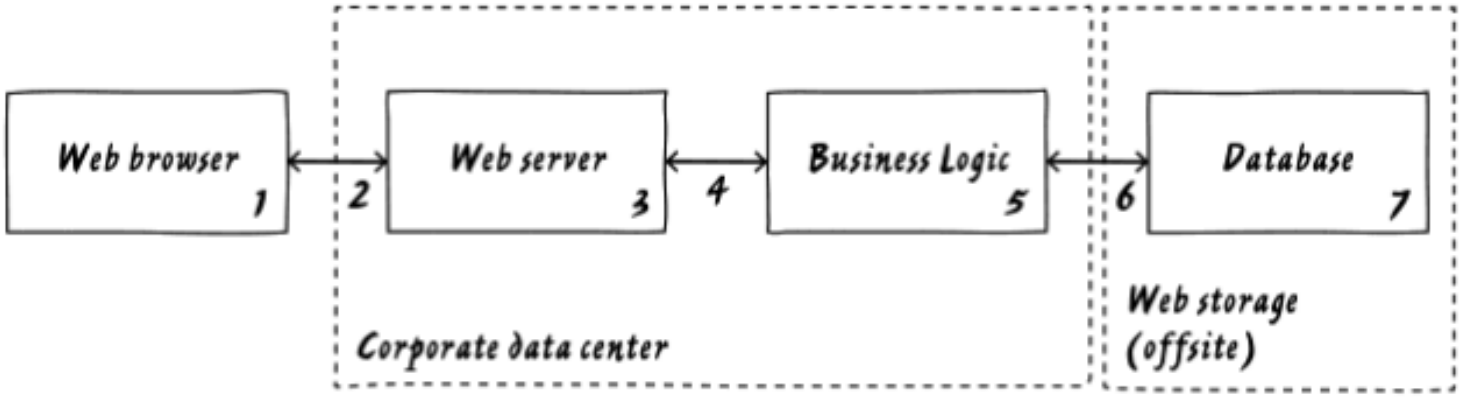


What can go wrong?
Where are the trust boundaries in this system?

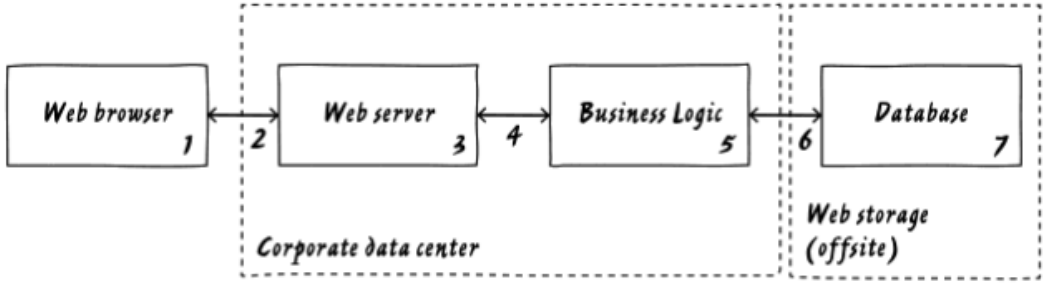
STRIDE

- Model of threats developed by Microsoft for identifying security architecture threats
- Is a mnemonic for 6 categories of threats:

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

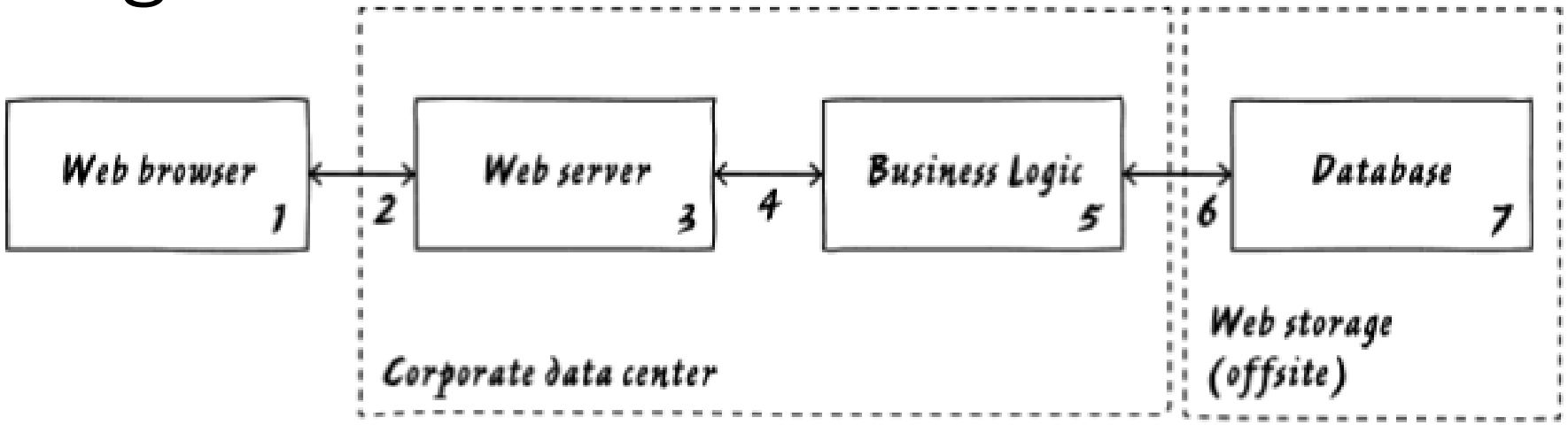


STRIDE



- **Spoofing** is pretending to be something or someone you are not
- **Tampering** is modifying something you are not supposed to modify
  - E.g. data packets in motion on the network, bits on disk, bits in memory…
- **Repudiation** means claiming you did not do something (regardless of whether you did or did not)
- **Information** Disclosure is exposing information to people who are not authorized to see it
- **Denial of Service** are attacks design to prevent the system's service availability
  - E.g. Crashing it, making it unusably slow, filling all of its storage, …

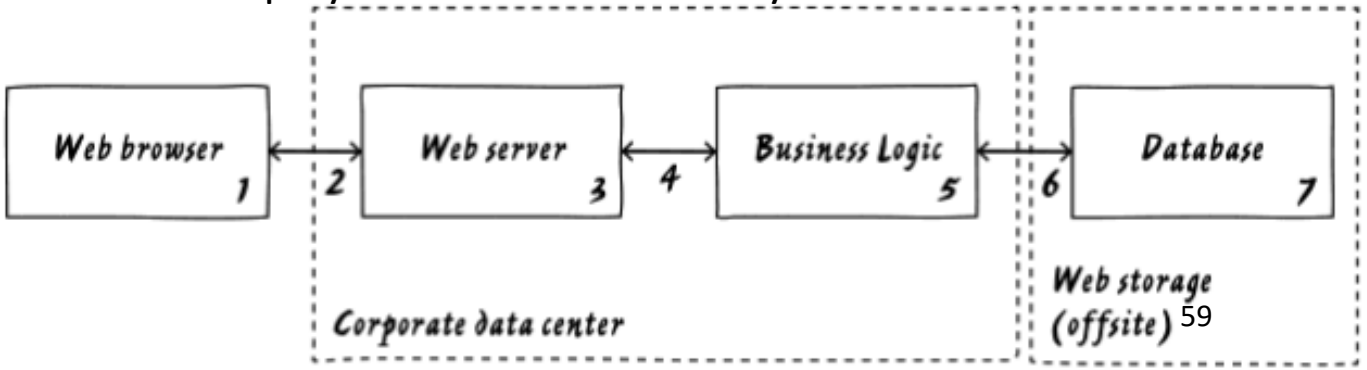
What can go wrong?



- How do you know the web browser is used by the person you expect?
- Is it OK for data to go from one box to the next without being encrypted?
- What happens if someone modified data in the database?

STRIDE – What can go wrong?

- **Spoofing:** Someone might pretend to be a customer, is there a way to authenticate users?
- **Tampering:** Can someone tamper with the data in the system's backend?
- **Repudiation:** Any preceding actions might require figuring out what happened
  - Are there system logs? Is the right information being logged? Are the logs protected against tampering?
- **Information Disclosure:** Can anyone connect to the database and read/write data?
- **Denial of Service:** What happens if 300,000 customers show up a once at the website?
  - What if the system goes down?
- **Elevation of Privileges:** Perhaps the web front end is the only place customers should access, but what enforces that?
  - What prevents them from connecting directly to the business logic server, or uploading new code?
  - What controls access to the database? What happens in an employee wants to edit the system files or makes a mistake?



Managing threats (i.e. managing risk)

- Avoid
- Accept
- Transfer
- Mitigate

Readings for next week…

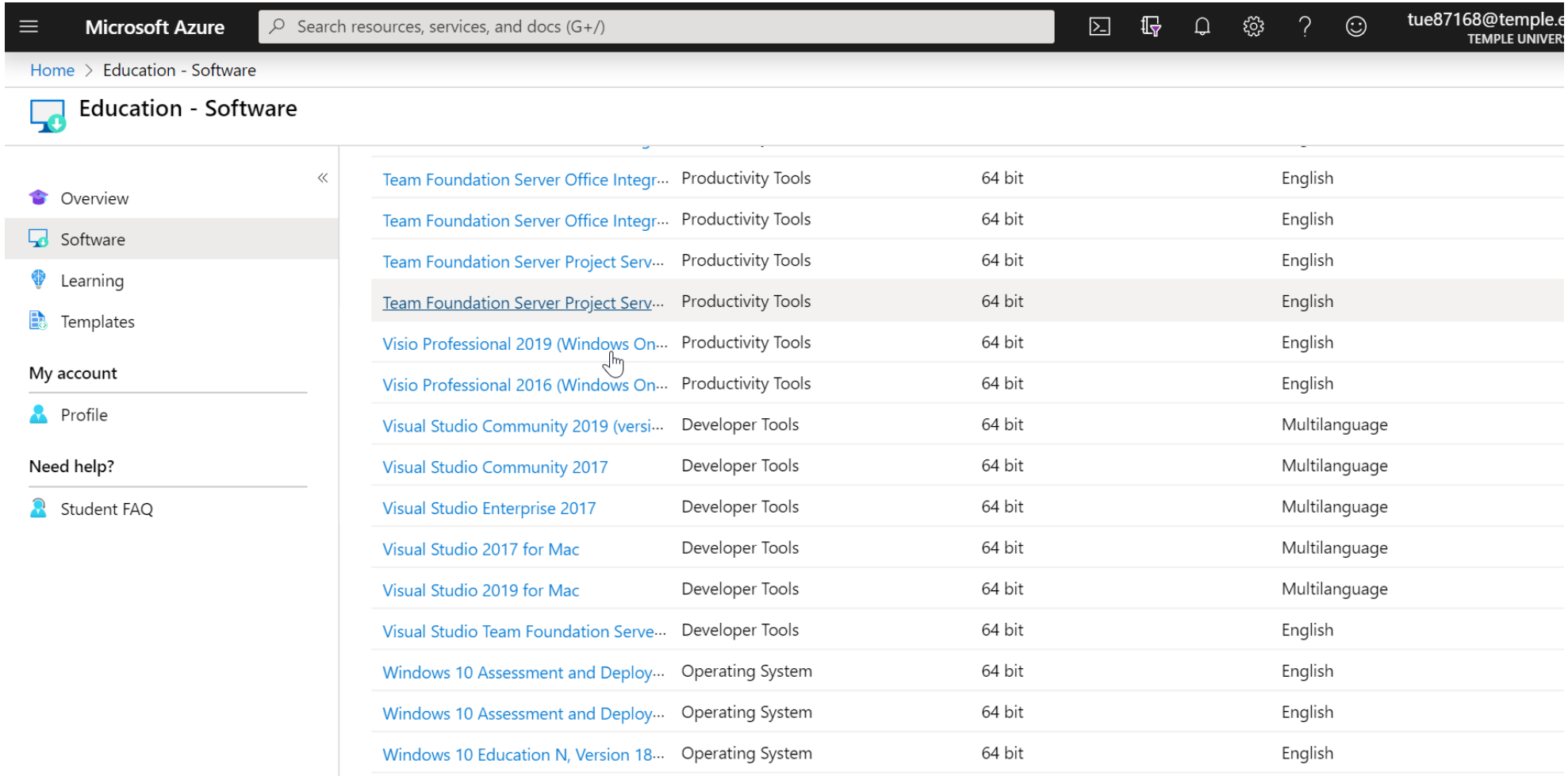
Unit 02 – System Security Plan

Readings

- NIST SP 800-100 “Information Security Handbook: A Guide for Managers”, Chapter 10 Risk Management, pp.84-95
- NIST SP 800-18r1 “Guide for Developing Security Plans for Federal Information Systems”
- “FedRAMP System Security Plan (SSP) High Baseline Template”

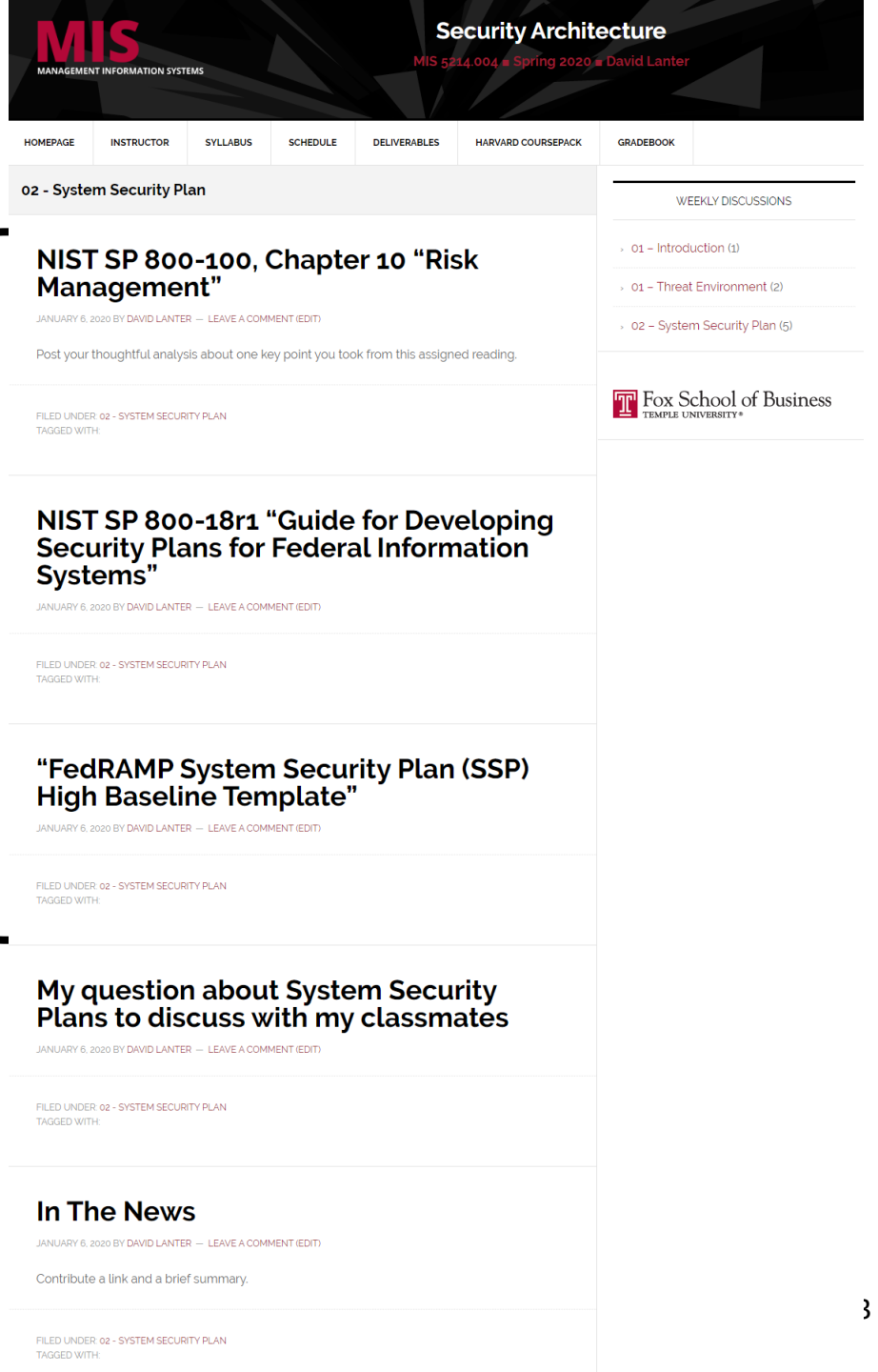
A useful tool for the course

Microsoft Azure education site



Questions for next week…

One Key Point Taken from Each Assigned Reading



Agenda

- ✓Welcome and Introductions
- ✓Course Introduction Goals
- ✓Introductory Terminology
- ✓The Threat Environment
- ✓Next Week…

Unit - #1

MIS5214 – Security Architecture