Unit - #1

MIS5214 – Security Architecture

Agenda

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

Course Goals – Security Architecture

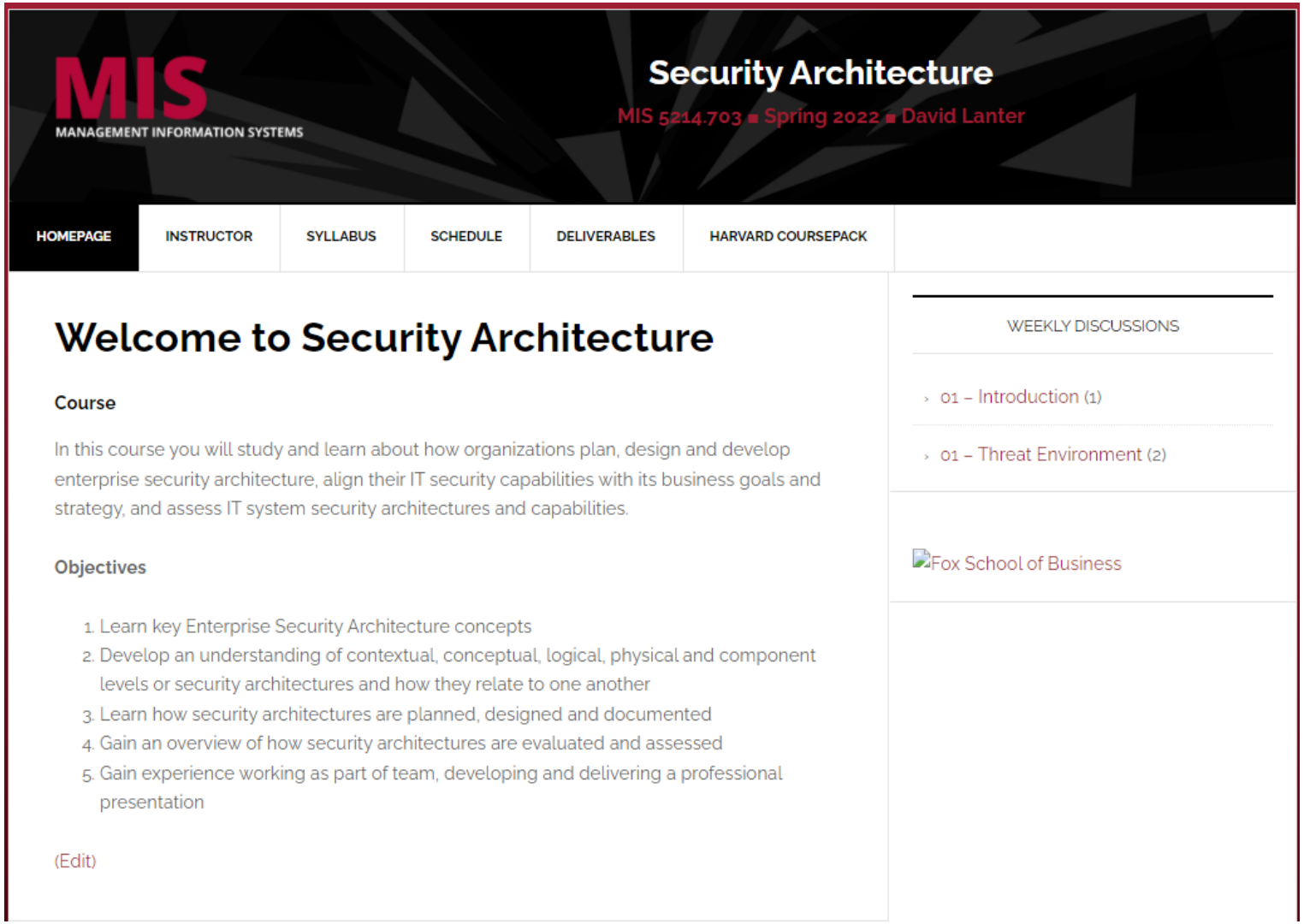
Learn about how organizations

- 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/mis5214sec703spring2022/welcome-to-security-architecture/

Instructor

David Lanter

Director - Information Technology Auditing and Cyber Security Programs

Philadelphia, Pennsylvania · 500+ connections · Contact info

Experience

Director - Information Technology Auditing and Cyber Security (ITACS) programs
Temple University – Fox School – Management Information Systems
Aug 2016 - Present · 5 yrs 6 mos
Greater Philadelphia Area

Vice President - Information Management Systems
CDM Smith
Sep 2001 - Aug 2016 · 15 yrs

Research Director
Rand McNally
Oct 1998 - Jun 2001 · 2 yrs 9 mos

GeoModeling QA Lead / Software Design Engineer
Microsoft
Oct 1996 - Jun 1998 · 1 yr 9 mos

President
Geographic Designs Inc.
Jan 1989 - Jun 1996 · 7 yrs 6 mos

Assistant Professor
University of California, Santa Barbara
Jan 1990 - Jun 1995 · 5 yrs 6 mos

Systems Analyst
Grumman Data Systems
Mar 1986 - Aug 1987 · 1 yr 6 mos

Software Engineer
Navigation Sciences
Jun 1985 - Jan 1986 · 8 mos
Bethesda, Maryland

Education

University of South Carolina
Ph.D., Geographic Information Processing
1987 – 1989

Temple University - Fox School of Business and Management
Master's Degree, IT Auditing and Cyber Security
2013 – 2015

State University of New York at Buffalo
Master's degree, Geographic Information Systems
1983 – 1986

Clark University
Bachelor's degree (with Honors), Science, Technology, and Society: Risk-Hazards/Computer Science
1981 – 1983

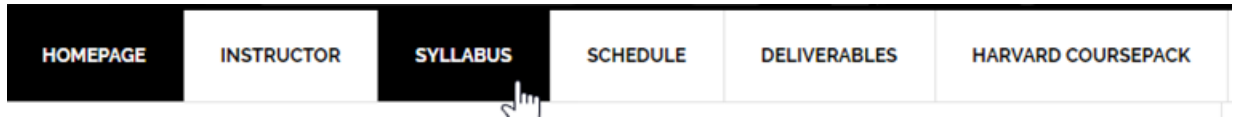
Licenses & certifications

Certified Information Systems Security Professional (CISSP)
(ISC)²
Issued Oct 2021 · No Expiration Date
Credential ID 586876

Certified Information Systems Auditor® (CISA)
ISACA
Issued Apr 2015 · No Expiration Date
Credential ID 15122708
See credential

GISP - Certified Geographic Information Systems Professional
GISCI
Issued Apr 2015 · No Expiration Date
Credential ID 30416
See credential

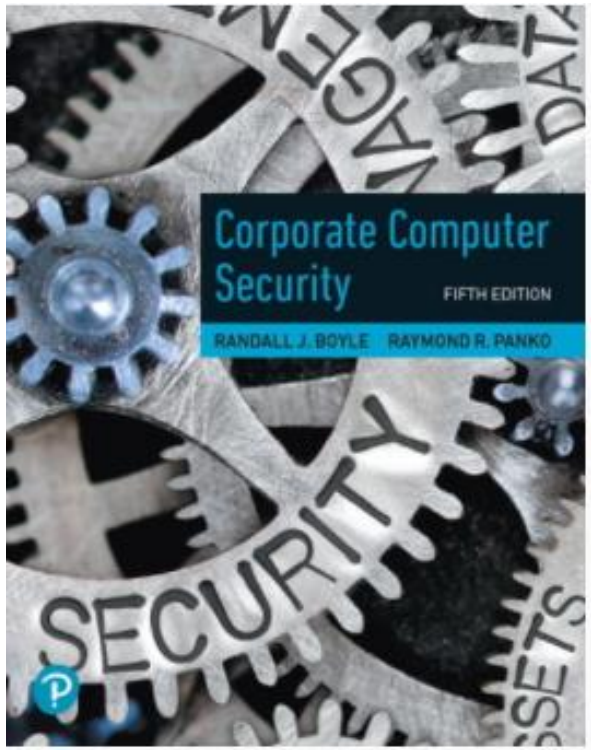
Syllabus


HOMEPAGE
INSTRUCTOR
SYLLABUS
SCHEDULE
DELIVERABLES
HARVARD COURSEPACK

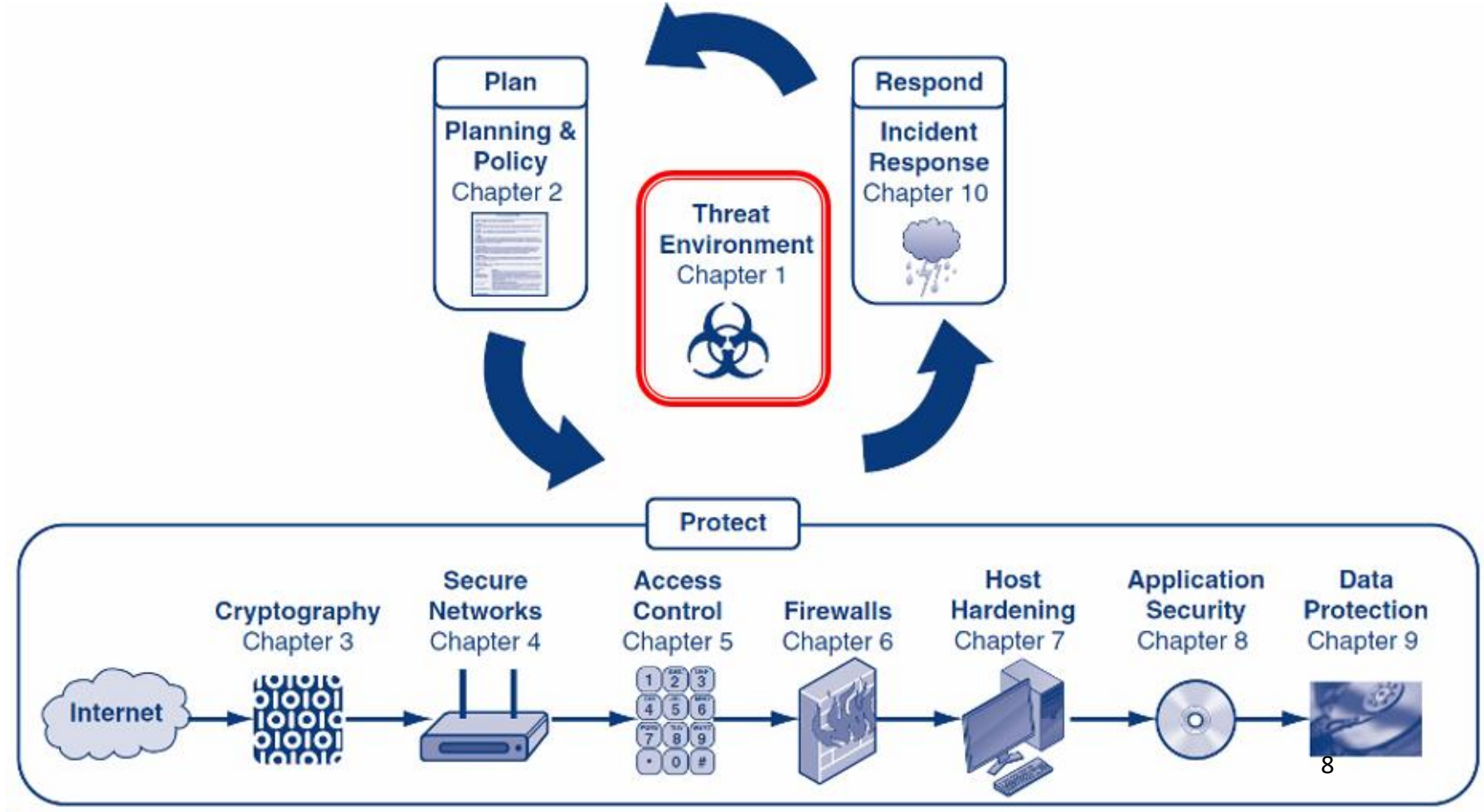
Textbook and Readings

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", pp. 18-26 • "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 • NIST SP 800-53r5 "Security and Privacy Controls for Information Systems and Organizations", pp.1-17 • NIST SP 800-53B "Control Baselines for Information Systems and Organizations", pp. 1-15 • NIST SP 800-53Ar4" Assessing Security and Privacy Controls for Federal Information and Information Systems", pp.1-28
4	• Boyle and Panko, Chapter 3 Cryptography • Case Study 1 "A High-Performance Computing Cluster Under Attack: The Titan Incident" (in the Harvard Business Publishing course pack)
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" • Case Study 2 "*Data Breach at Equifax*" (in the Harvard Business Publishing course pack)
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, Introduction • How to use the OWASP Top 10 as a standard • How to start an AppSec program with 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



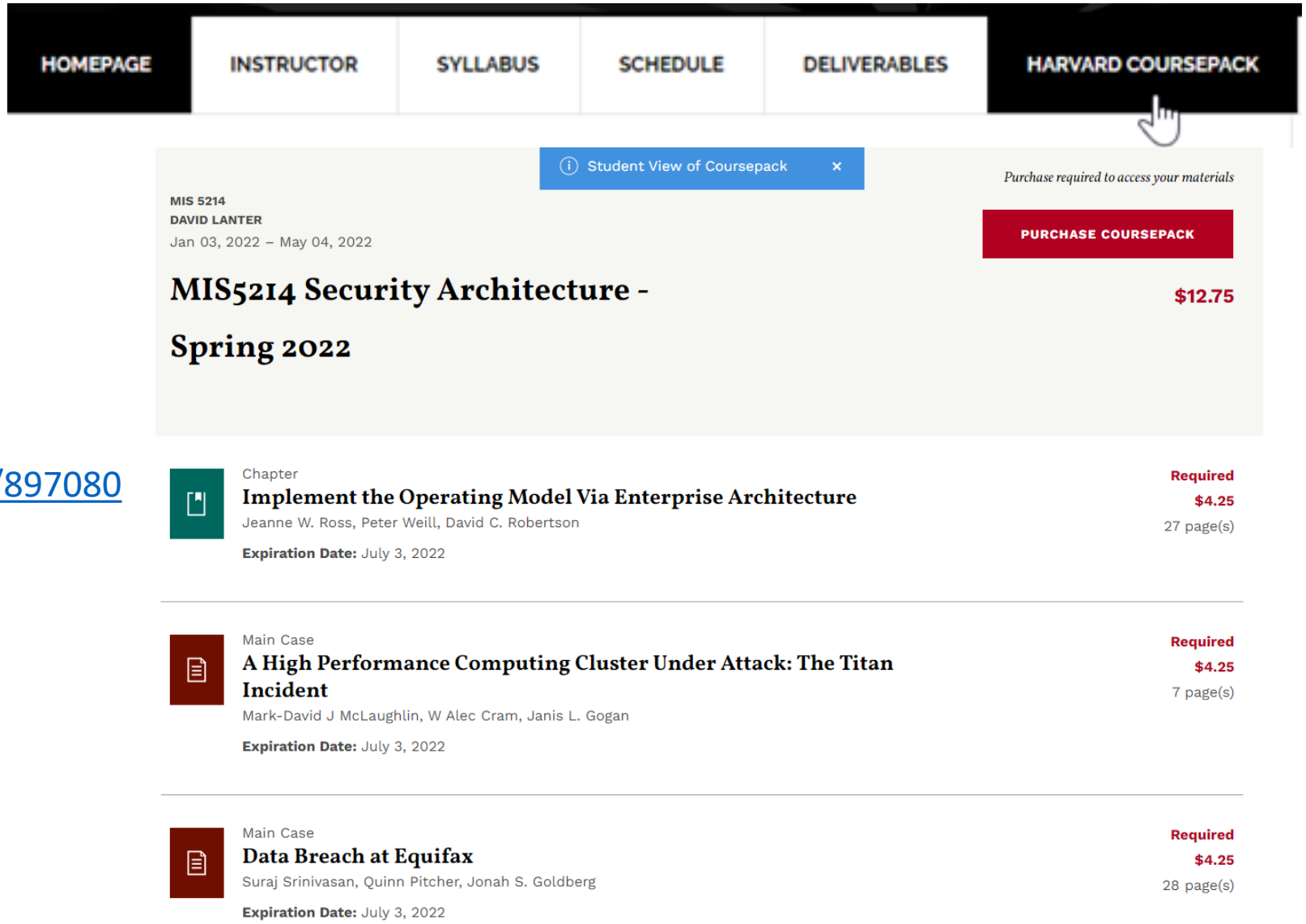
How is this book organized?



Harvard Business Publishing Course Pack

- 1 Reading
- 2 Case Studies

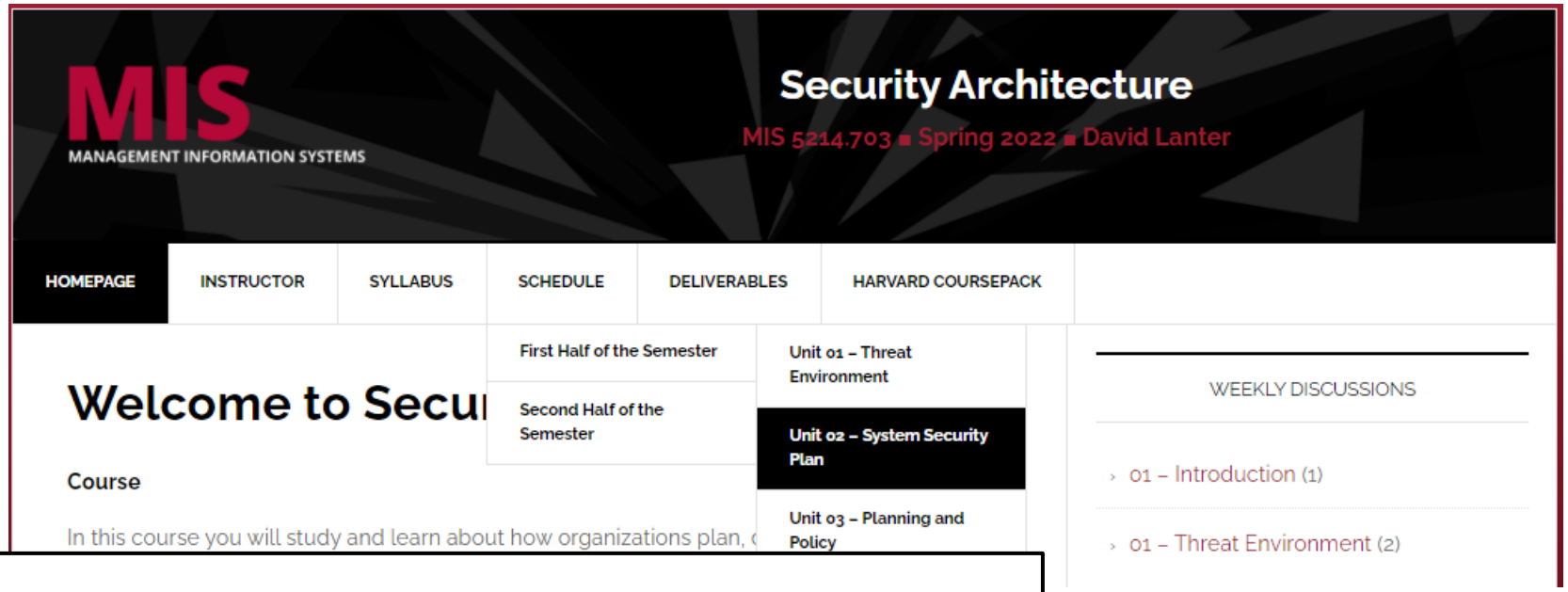
https://hbsp.harvard.edu/import/897080



Class Schedule

Unit #	Topics	Date
1	Introduction	1/12
	The Threat Environment	
2	System Security Plan	1/19
3	Planning and Policy	1/26
4	Case Study 1 "*A High-Performance Computing Cluster Under Attack: The Titan Incident*"	2/2
	Cryptography	
5	Secure Networks	2/9
6	Firewalls, Intrusion Detection and Protection Systems	2/16
7	**Mid-Term Exam**	2/23
	Spring Break	3/2
8	Case Study 2 "*Data Breach at Equifax*"	3/9
	Access Control	
9	Host Hardening	3/16
10	Application Security	3/23
11	Data Protection	3/30
12	Incident and Disaster Response	4/6
13	Team Project Presentations	4/13
14	Team Project Presentations	4/20
	Course Review	
	Final Exam	5/4

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	25%
Participation	25%
Team Project	25%
Exams	25%
	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 - 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

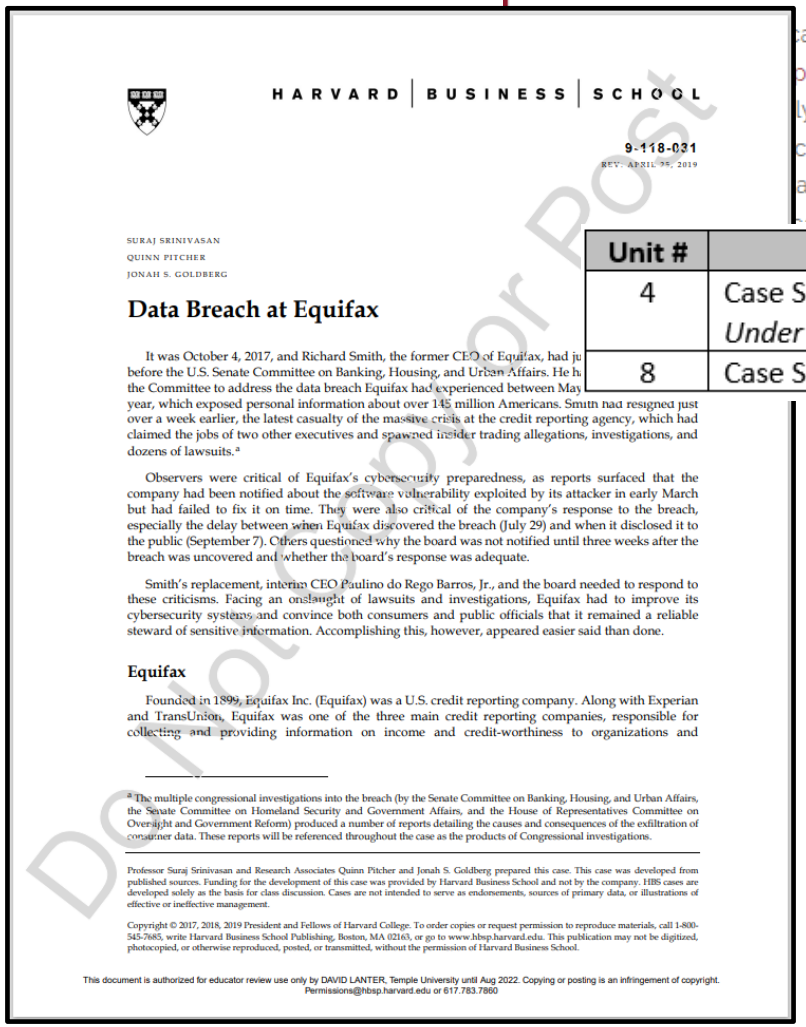
Keywords: information security; incident response; risk management; inter-organizational collaboration; IT governance; high performance computing

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



HARVARD | BUSINESS | SCHOOL

9-118-031
REV. APRIL 25, 2019

SURAJ SRINIVASAN
QUINN PITCHER
JONAH S. GOLDBERG

Data Breach at Equifax

It was October 4, 2017, and Richard Smith, the former CEO of Equifax, had ju
before the U.S. Senate Committee on Banking, Housing, and Urban Affairs. He h
the Committee to address the data breach Equifax had experienced between May
year, which exposed personal information about over 145 million Americans. Smith had resigned just over a week earlier, the latest casualty of the massive crisis at the credit reporting agency, which had claimed the jobs of two other executives and spawned insider trading allegations, investigations, and dozens of lawsuits.[a]

Observers were critical of Equifax's cybersecurity preparedness, as reports surfaced that the company had been notified about the software vulnerability exploited by its attacker in early March but had failed to fix it on time. They were also critical of the company's response to the breach, especially the delay between when Equifax discovered the breach (July 29) and when it disclosed it to the public (September 7). Others questioned why the board was not notified until three weeks after the breach was uncovered and whether the board's response was adequate.

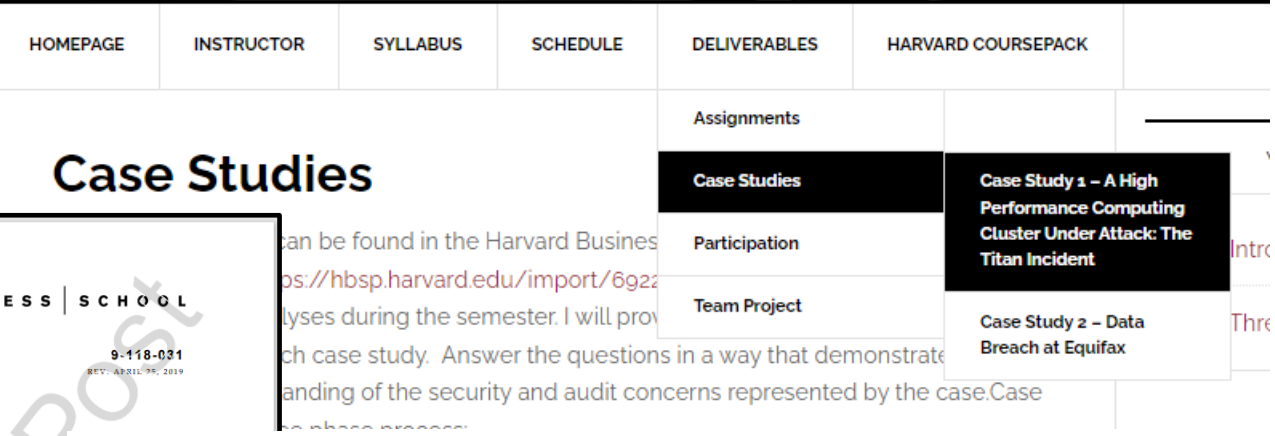
Smith's replacement, interim CEO Paulino do Rego Barros, Jr., and the board needed to respond to these criticisms. Facing an onslaught of lawsuits and investigations, Equifax had to improve its cybersecurity systems and convince both consumers and public officials that it remained a reliable steward of sensitive information. Accomplishing this, however, appeared easier said than done.

Equifax

Founded in 1899, Equifax Inc. (Equifax) was a U.S. credit reporting company. Along with Experian and TransUnion, Equifax was one of the three main credit reporting companies, responsible for collecting and providing information on income and credit-worthiness to organizations and

[a] The multiple congressional investigations into the breach (by the Senate Committee on Banking, Housing, and Urban Affairs, the Senate Committee on Homeland Security and Government Affairs, and the House of Representatives Committee on Oversight and Government Reform) produced a number of reports detailing the causes and consequences of the exfiltration of consumer data. These reports will be referenced throughout the case as the products of Congressional investigations.

Professor Suraj Srinivasan and Research Associates Quinn Pitcher and Jonah S. Goldberg prepared this case. This case was developed from published sources. Funding for the development of this case was provided by Harvard Business School and not by the company. HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.



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

Assignments

Case Studies

Participation

Team Project

Case Study 1 – A High Performance Computing Cluster Under Attack: The Titan Incident

Case Study 2 – Data Breach at Equifax

Case Studies

an be found in the Harvard Busines
ps://hbsp.harvard.edu/import/692
lyses during the semester. I will prov
ch case study. Answer the questions in a way that demonstrate
anding of the security and audit concerns represented by the case.Case

Unit #	Case Study	Due	Discussion
4	Case Study 1: "*A High-Performance Computing Cluster Under Attack: The Titan Incident*"	1/30	2/2
8	Case Study 2: "*Data Breach at Equifax*"	3/6	3/9

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 Rough Draft System Security Plan (SSP) review	3/23
10	2nd Draft SSP review	3/30
11	3rd Draft SSP review	4/6
12	Presentation of Final Deliverables	4/13
13	Presentation of Final Deliverables	4/20

Grading - Exams

Unit #	Exam	Date
7	Mid-Term	3/3
	Final	5/4

Weekly Cycle

When	Actor	Task	Type
Thursday	Instructor	Post readings & assignment questions	Assignment
Sunday midnight	Student	Post key points from readings, question for classmates	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…
  1. Access, use, disclosure = **Confidentiality**
  2. Modification or distruction = **Integrity**
  3. Disruption or loss of access = **Availability**

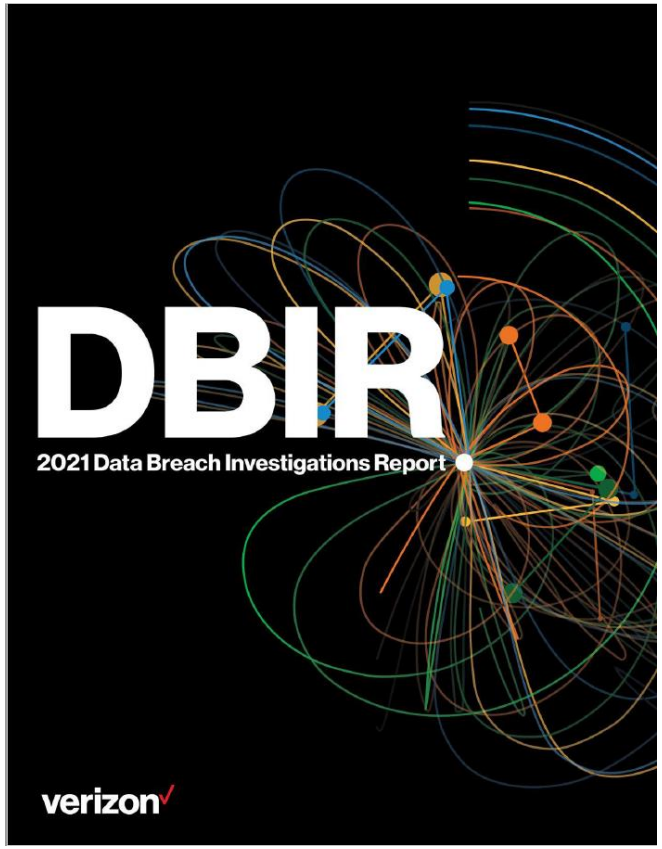
Terminology: Compromises

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

Terminology: Countermeasures

- Tools used to thwart attacks
- Also called: safeguards, protections, mitigations and controls
- Types of countermeasures:
  - **Preventative controls**
    - For reducing risk
    - Deterrent controls – preventative controls for discouraging violations
  - **Detective controls**
    - For identifying violations and incidents
  - **Corrective controls**
    - Attempt to reverse the impact of an incident
  - **Compensating controls**
    - Alternative controls when a primary control is not feasible

Threat Environment



Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

Table 4. Number of security incidents and breaches by victim industry and organization size

Based on analysis of 29,207 security incidents, of which 5,258 were confirmed data breaches

Threat Environment

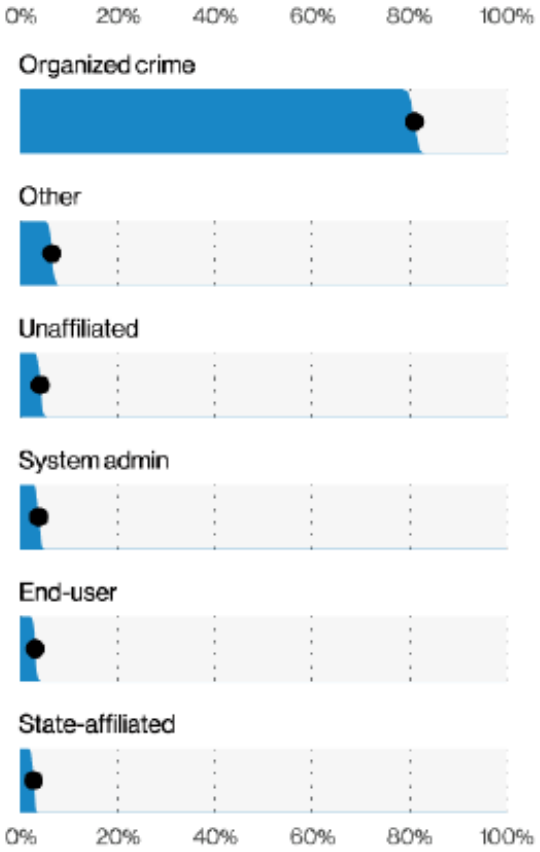


Figure 16. Top threat actor varieties in breaches (n=2,277)

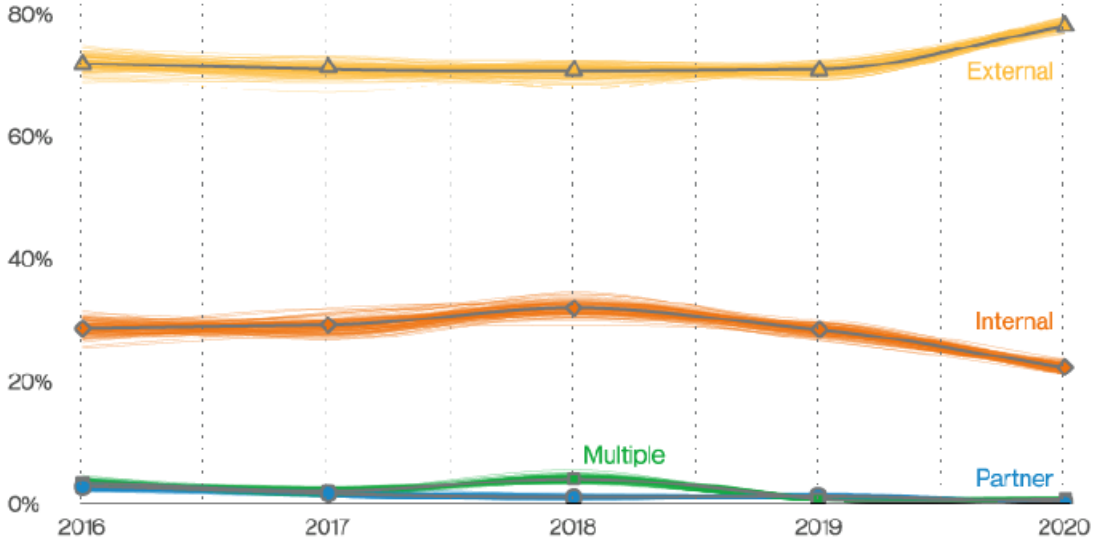


Figure 14. Threat actor over time in breaches

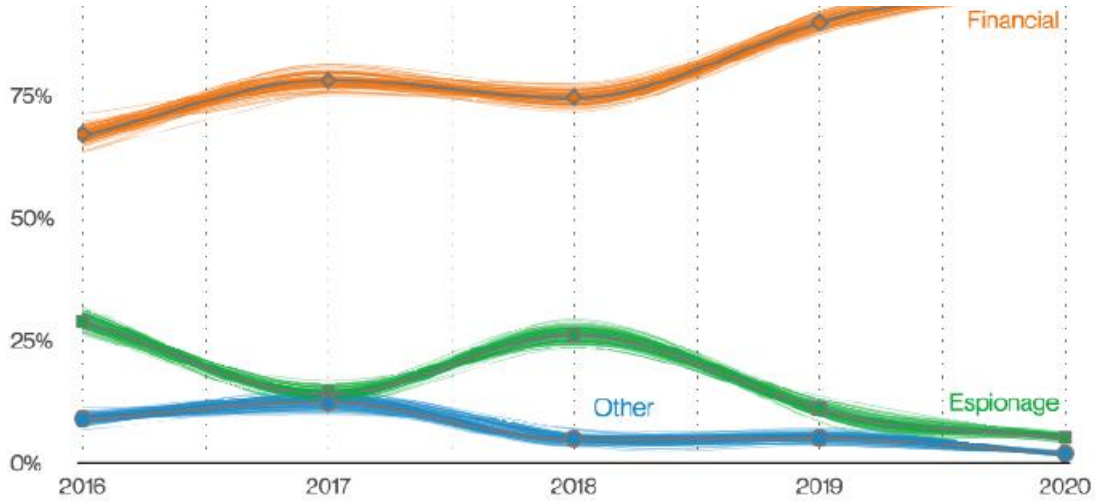
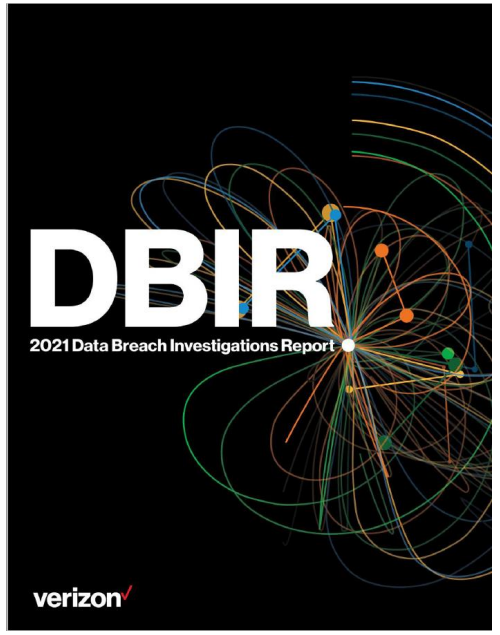


Figure 15. Top threat actor motive over time in breaches



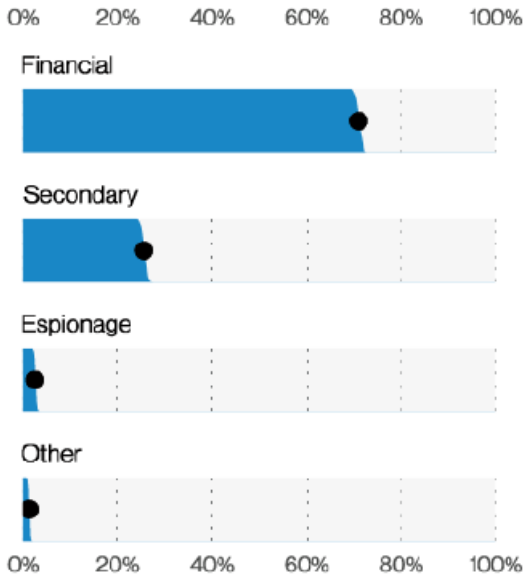
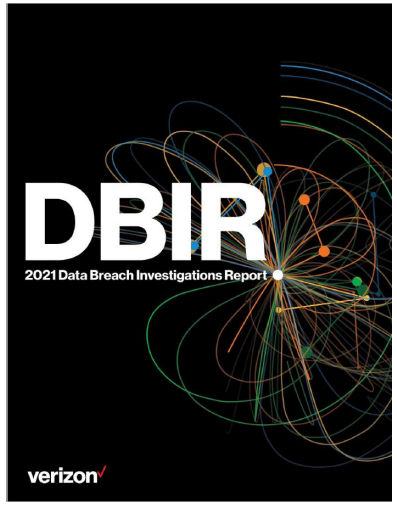


Figure 18. Top Actor motives in incidents (n=5,085)

Threat Environment



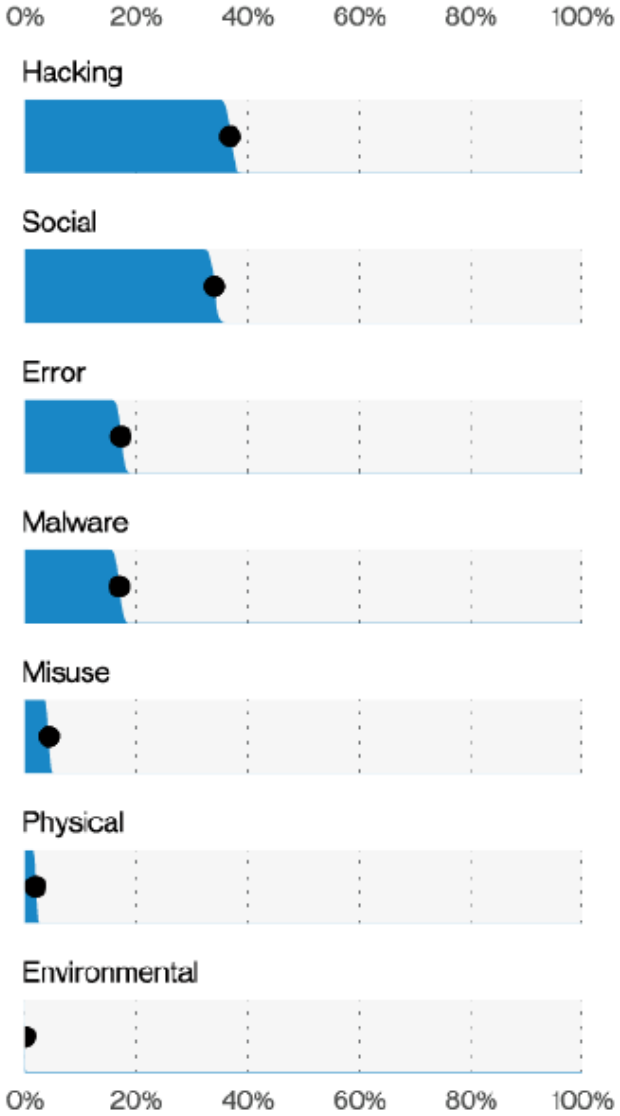


Figure 23. Actions in breaches (n=5,257)

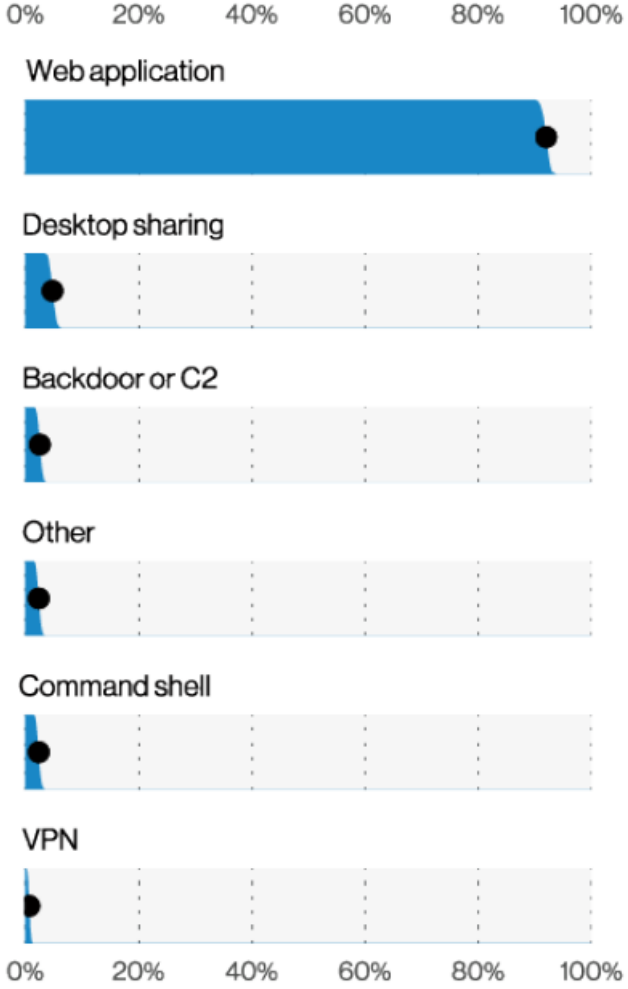
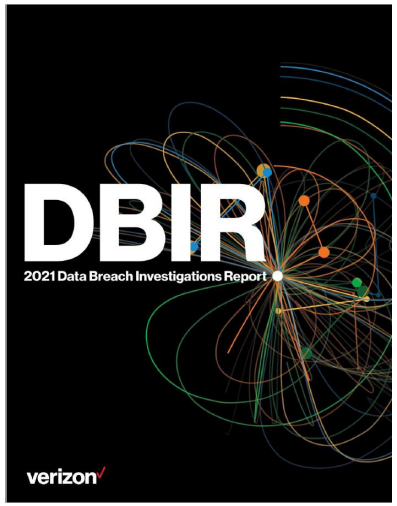


Figure 26. Top Hacking vectors in breaches (n=1,610)

Threat Environment



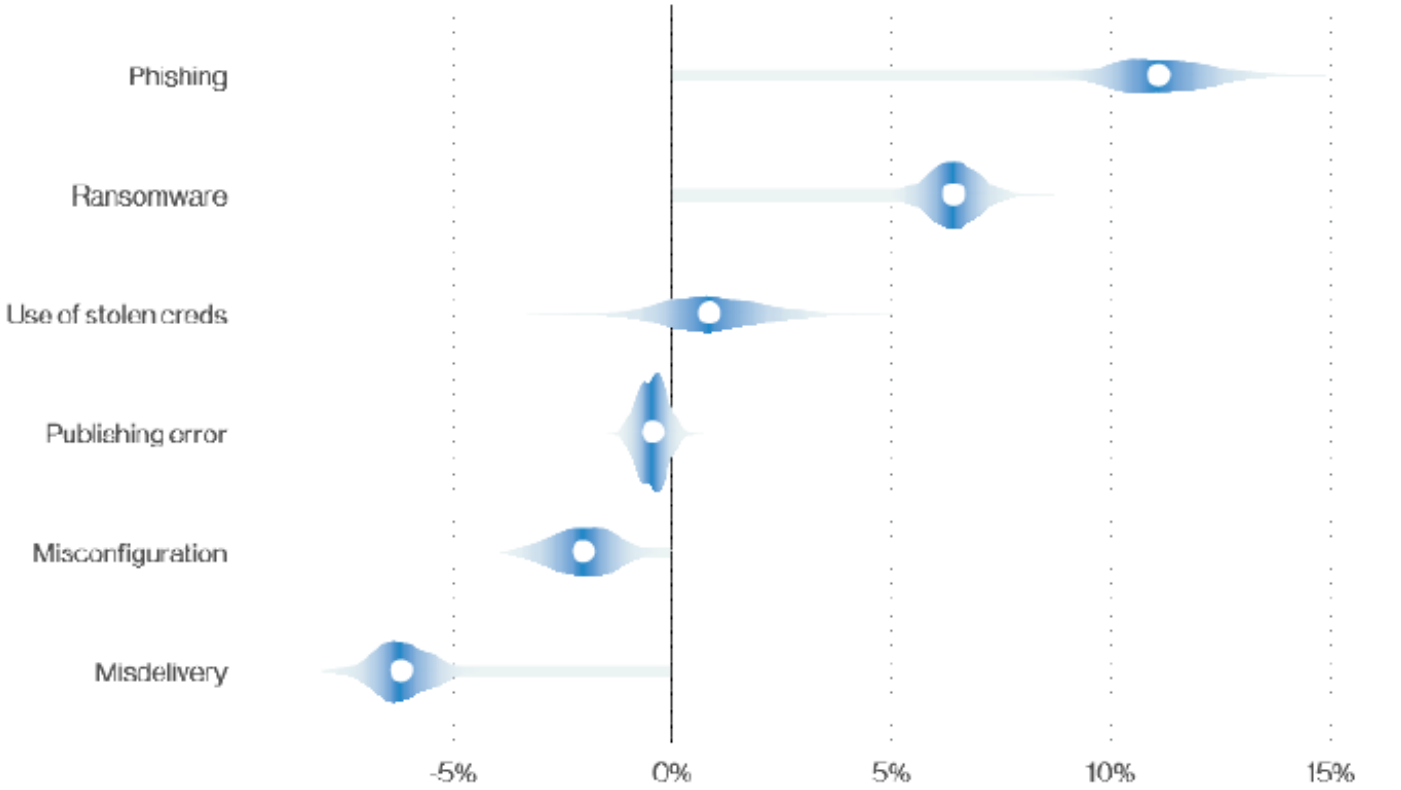
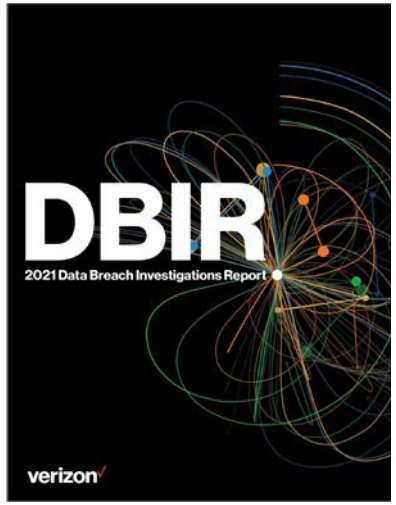


Figure 22. Change in COVID-19-related Action varieties

Threat Environment



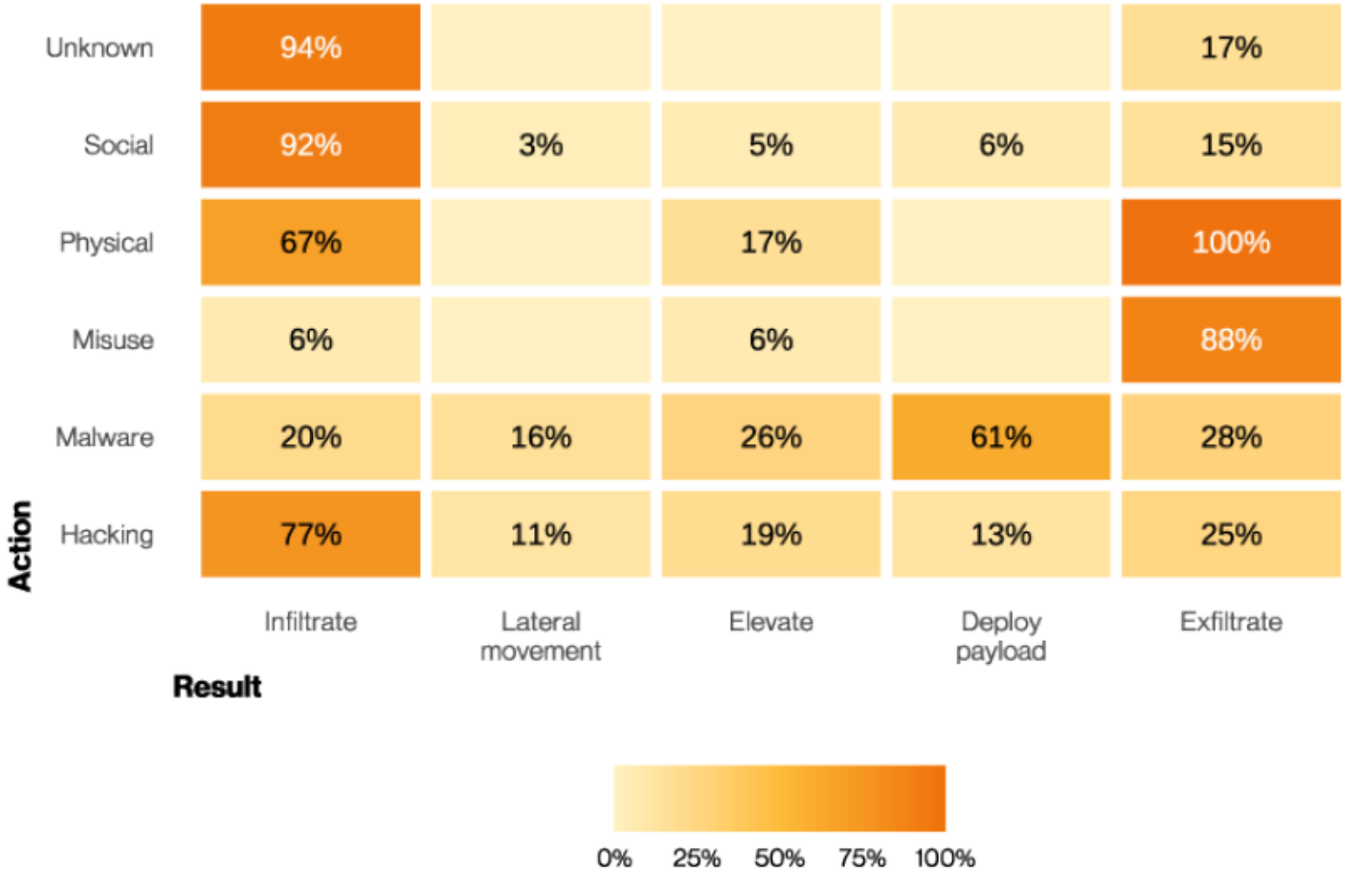
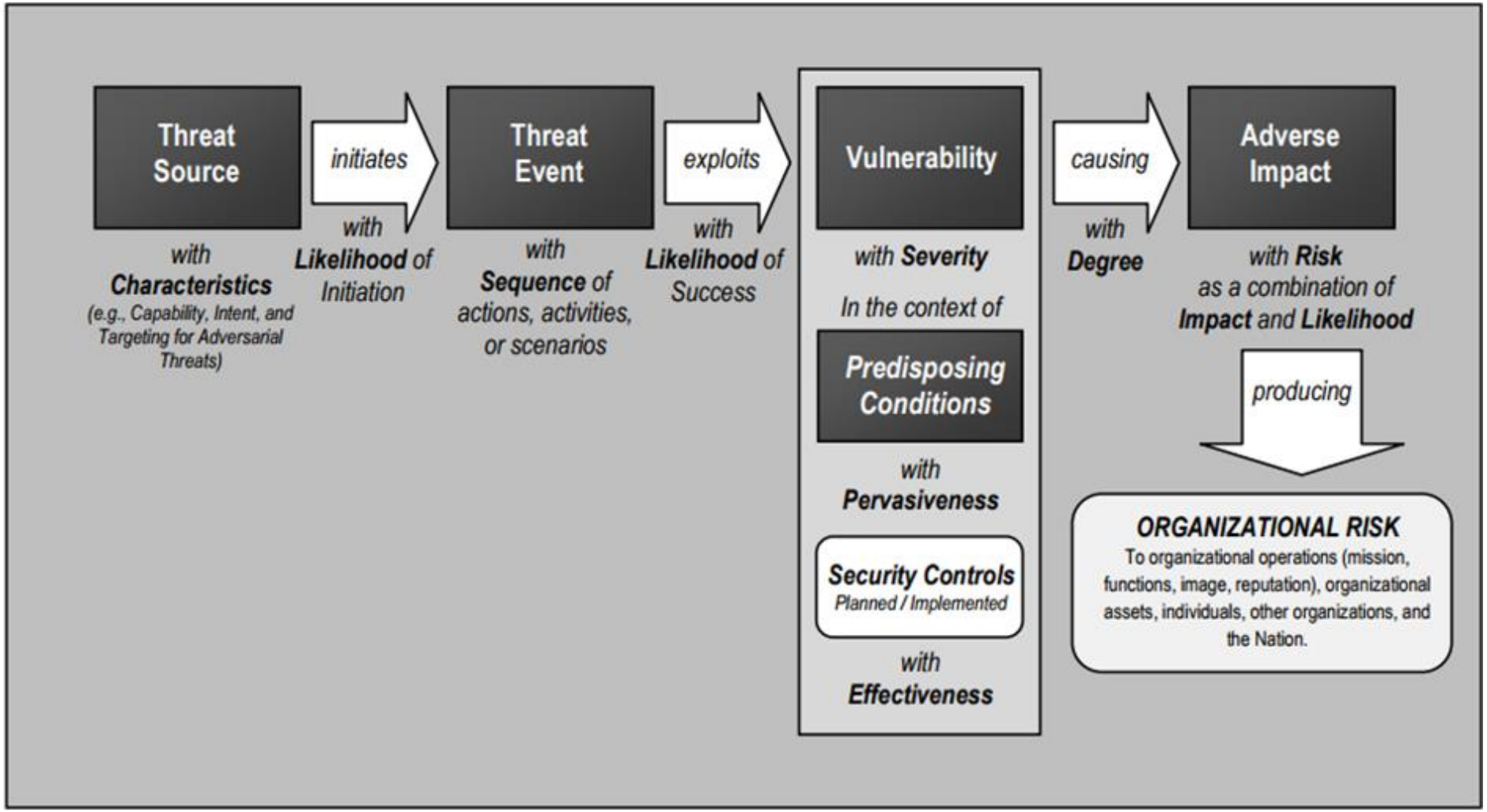


Figure 24. Results in breach Actions

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

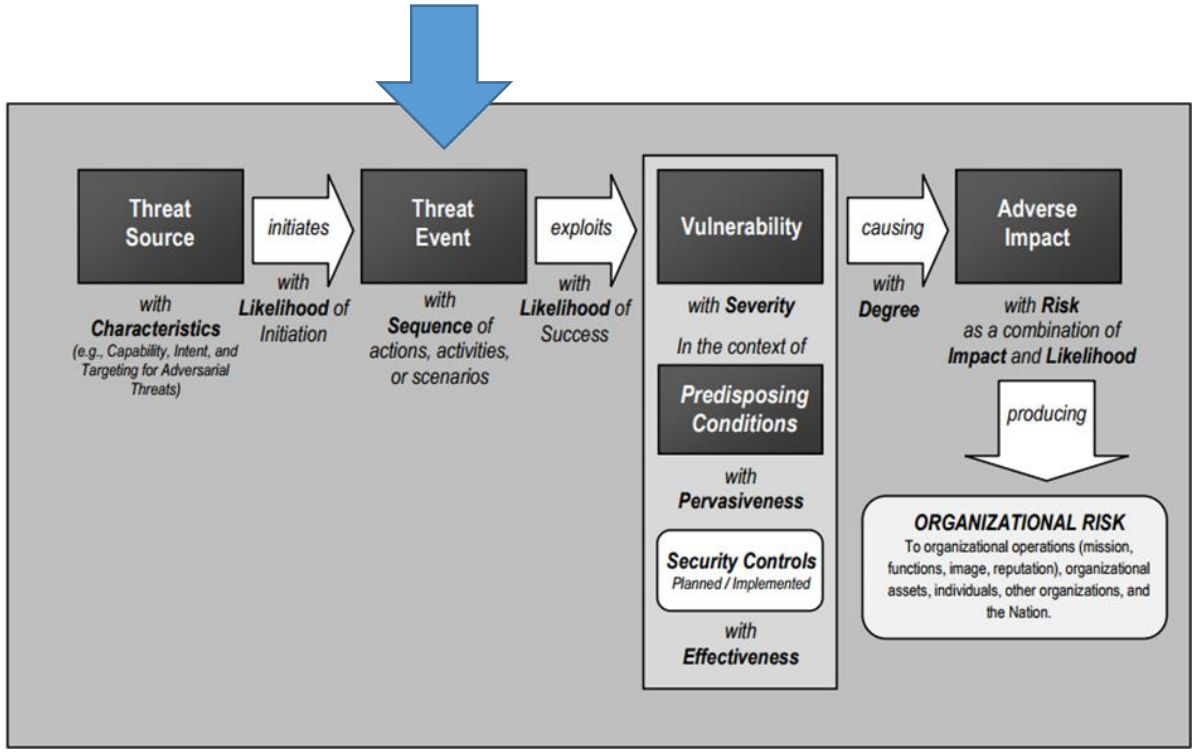
The Secret to Hacking

"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



Breaches

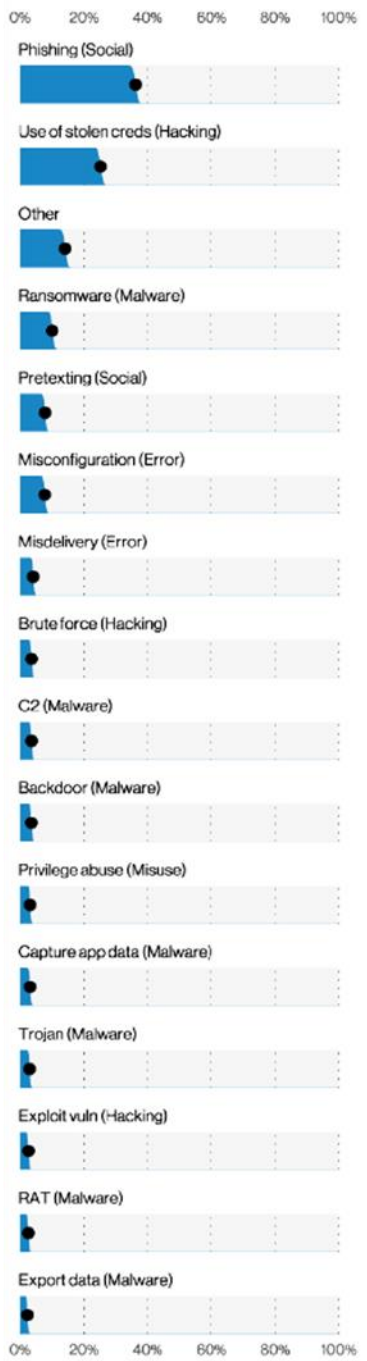


Figure 20. Top Action varieties in breaches (n=4,073)

Incidents

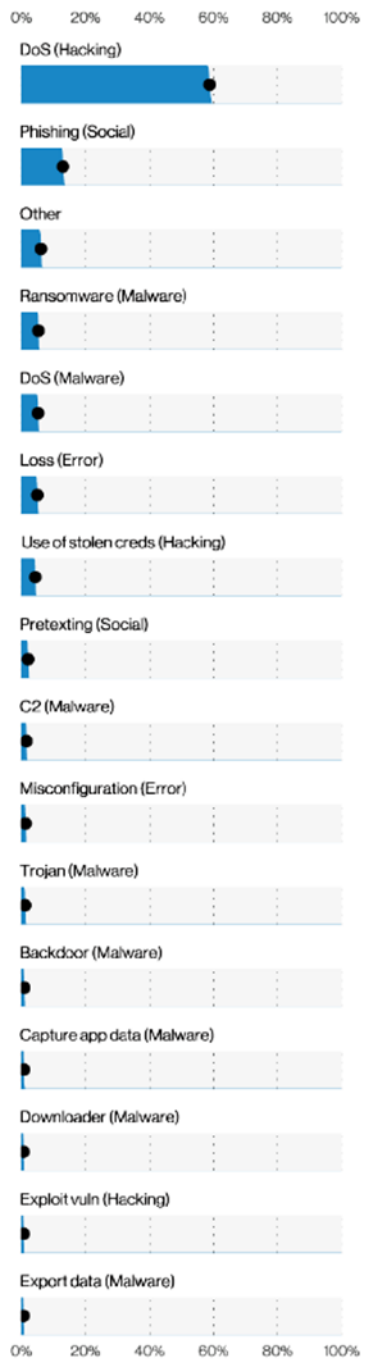
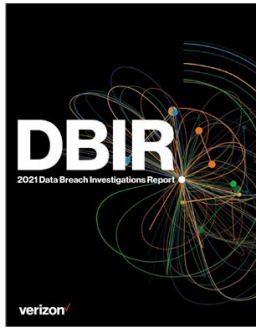


Figure 21. Top Action varieties in incidents (n=24,362)

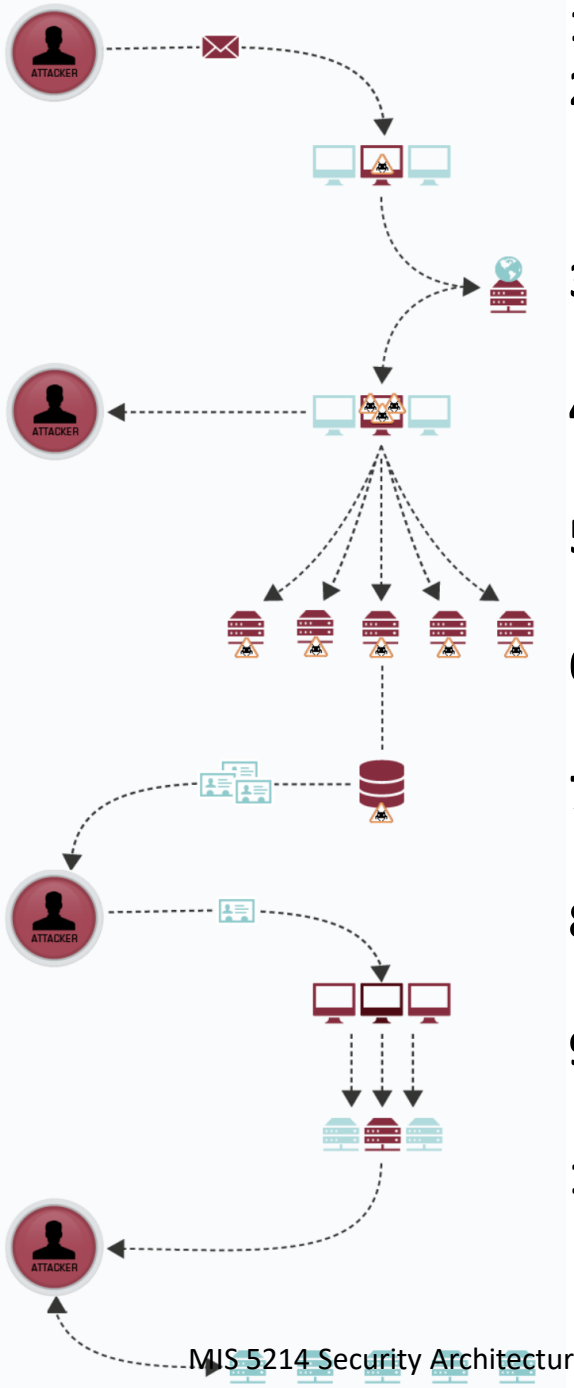
C2 = Command & Control malware

RAT = Remote Access Trojan



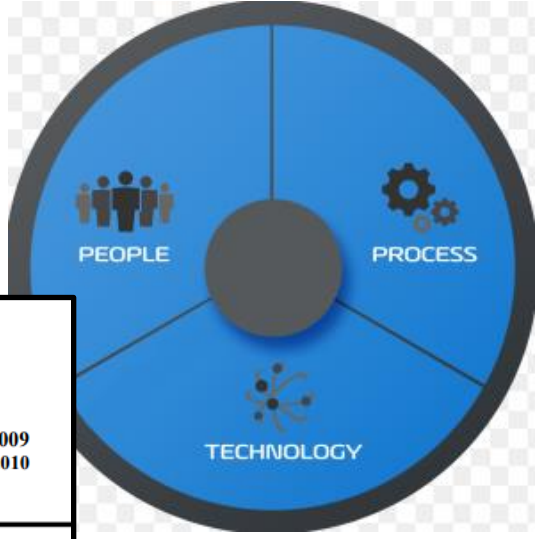
Anatomy of an Attack

(MANDIANT, 2015)

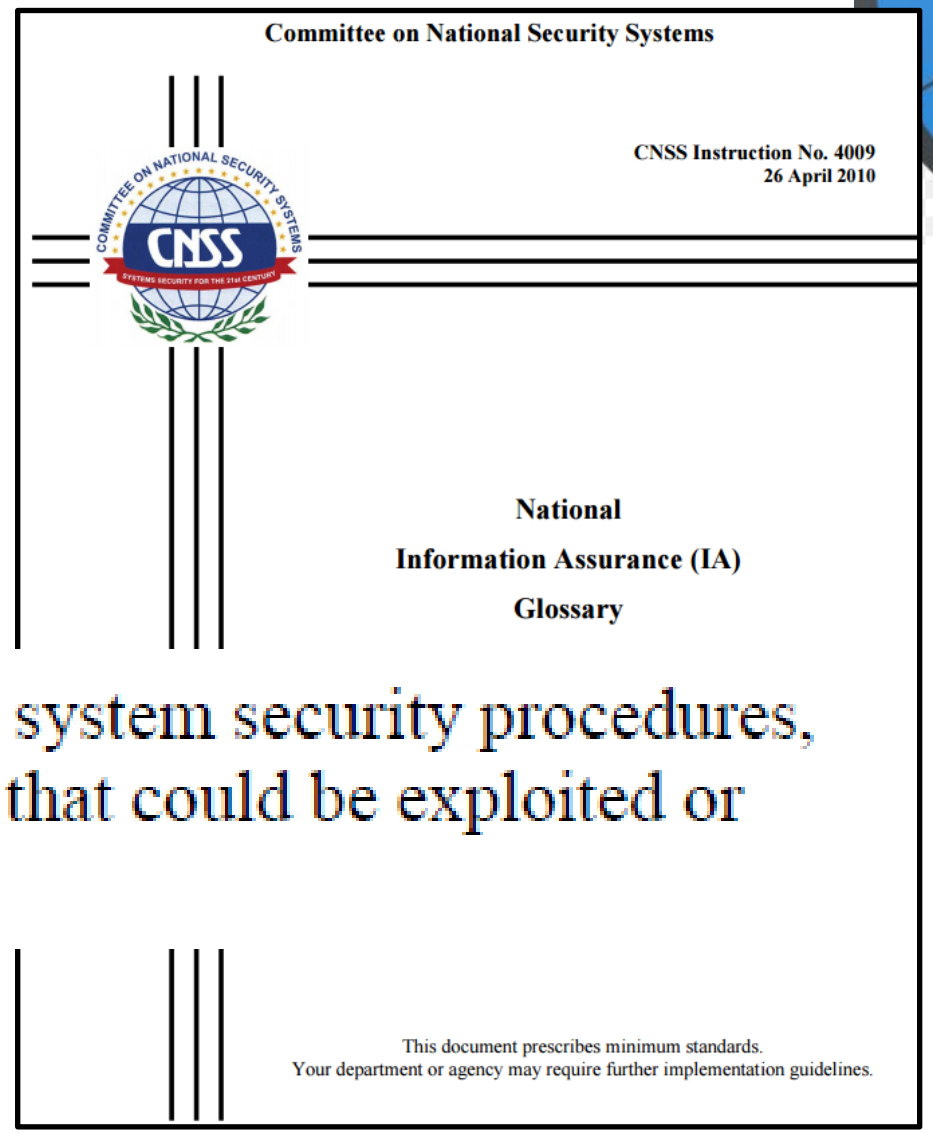


1. **Attacker sends spear phishing e-mail**
2. **Victim opens attachment**
   - Custom malware is installed
3. **Custom malware communicates to control web site**
   - Pulls down additional malware
4. **Attacker establishes multiple backdoors**
5. **Attacker accesses system**
   - Dumps account names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

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
  - Employees – inadequate screening and recruiting process, lack of security awareness and training
  - Business Processes – Lack of regular audits
  - Disaster Recovery Plans – 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:

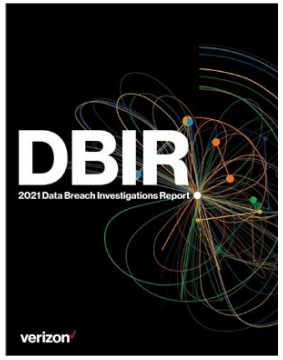
- *Access, use, disclosure*
- *Modification*
- *Disruption or destruction*

…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 ?



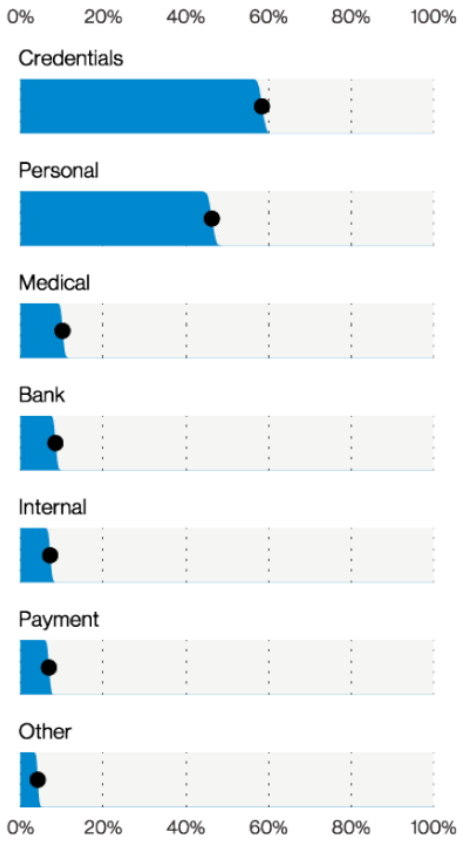


Figure 35. Top data varieties in breaches (n=4,552)

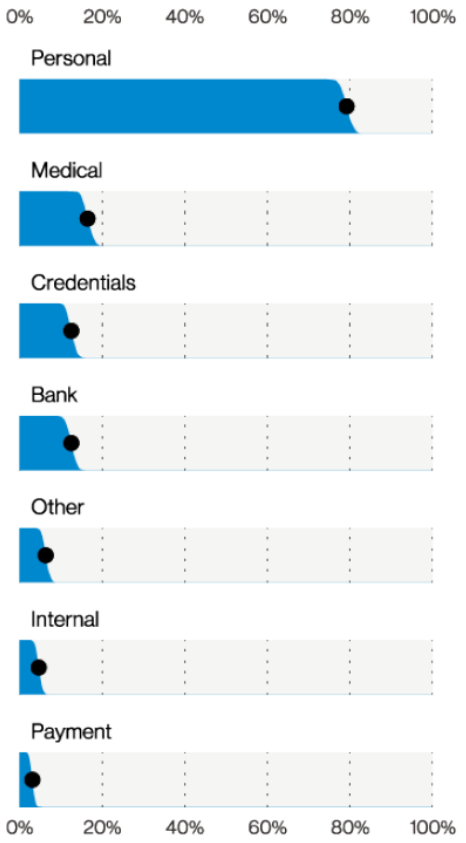


Figure 36. Top data varieties in Error breaches (n=839)

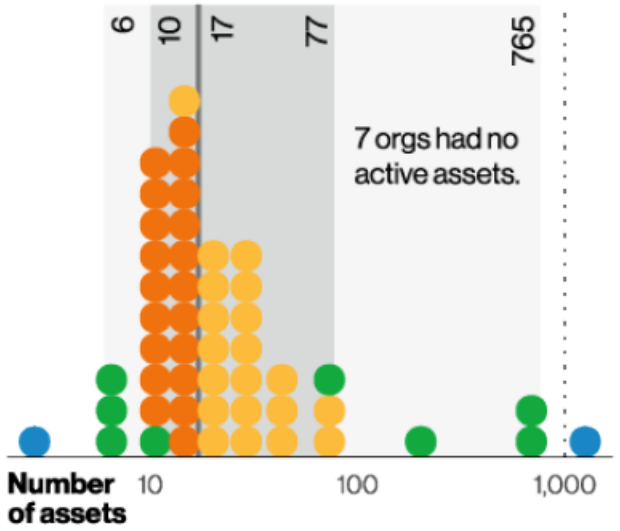
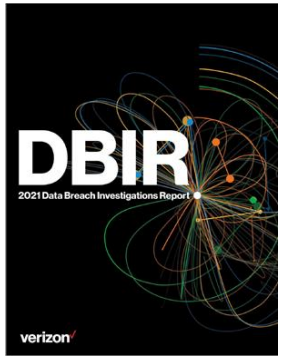


Figure 30. Number of internet-facing assets in randomly selected organizations (n=85) Each dot represents 2% of organizations

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 ?



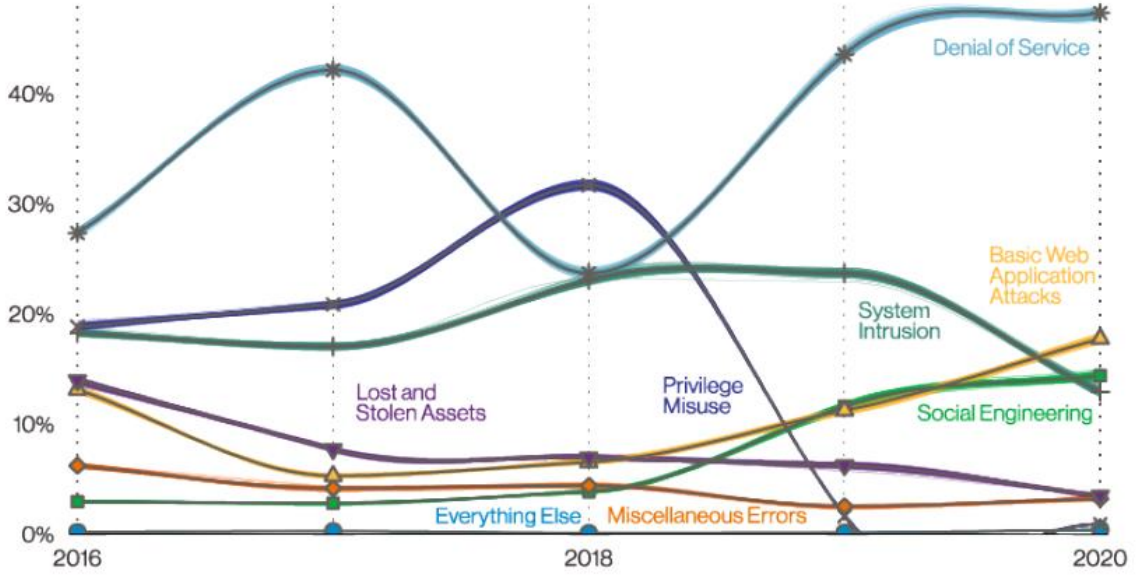


Figure 44. Patterns over time in incidents

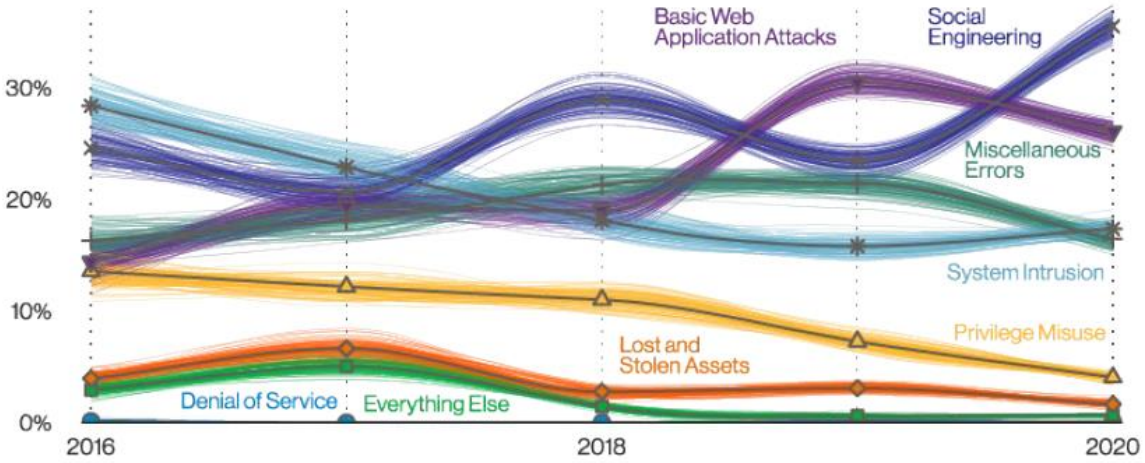


Figure 45. Patterns over time in breaches

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**

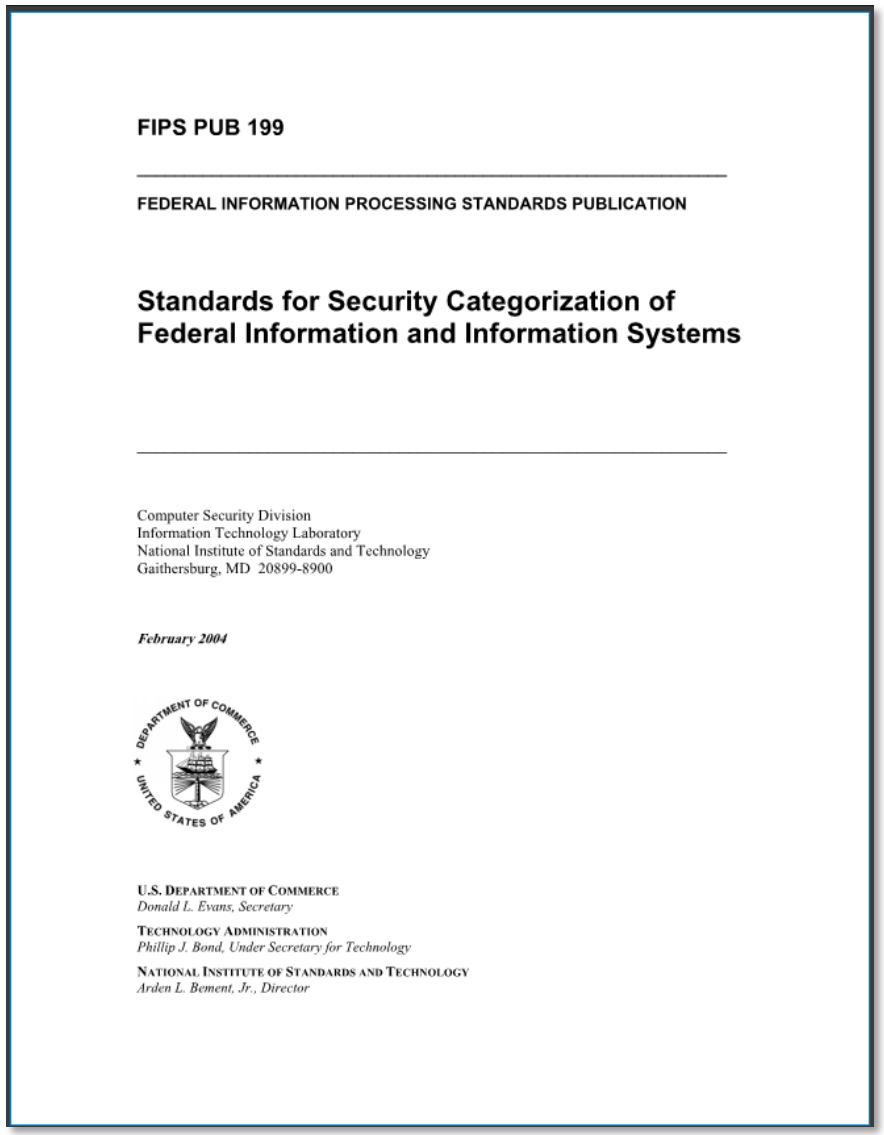
   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

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

	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
- Information systems’ security

…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

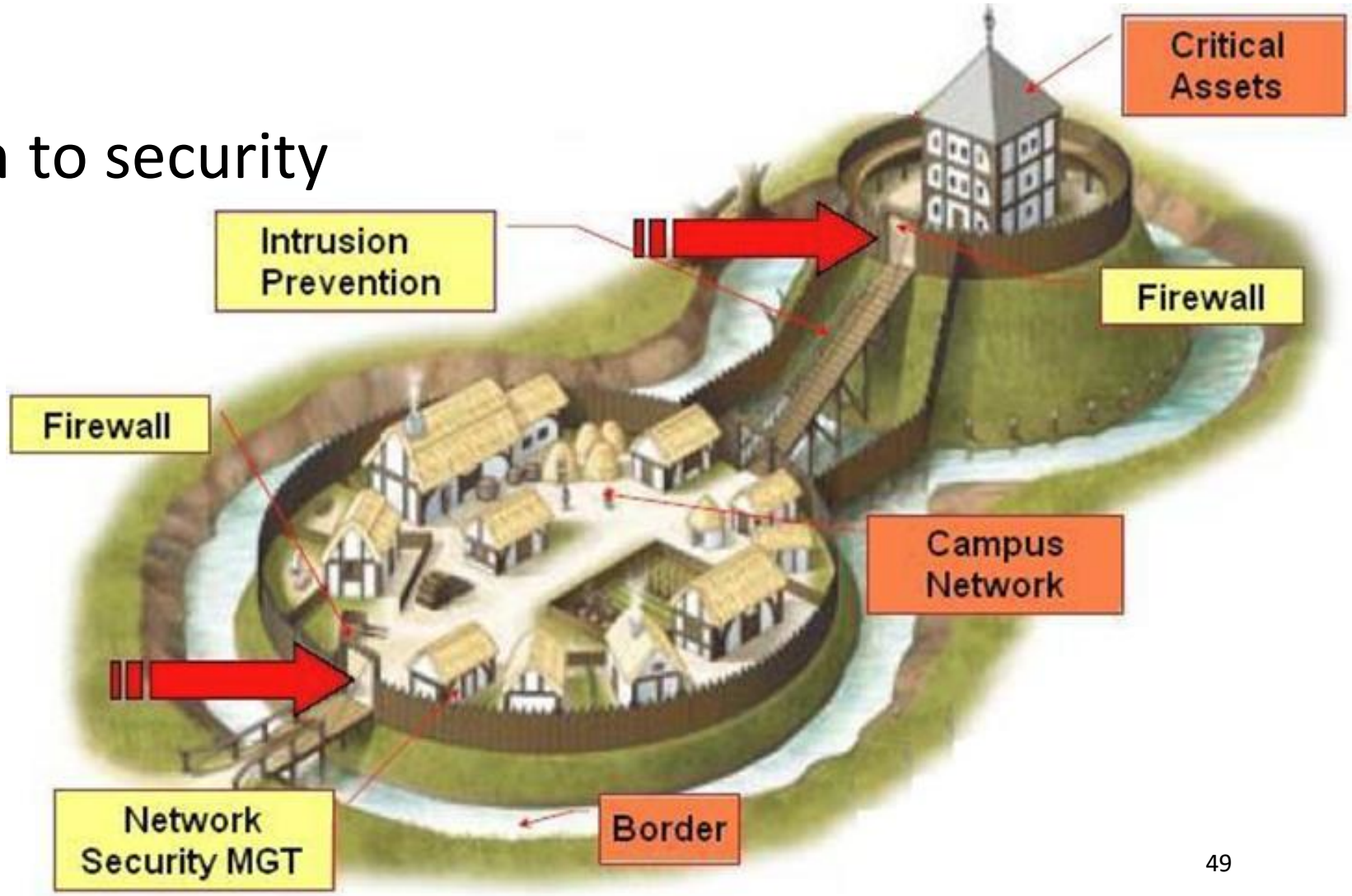
Security Architecture

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

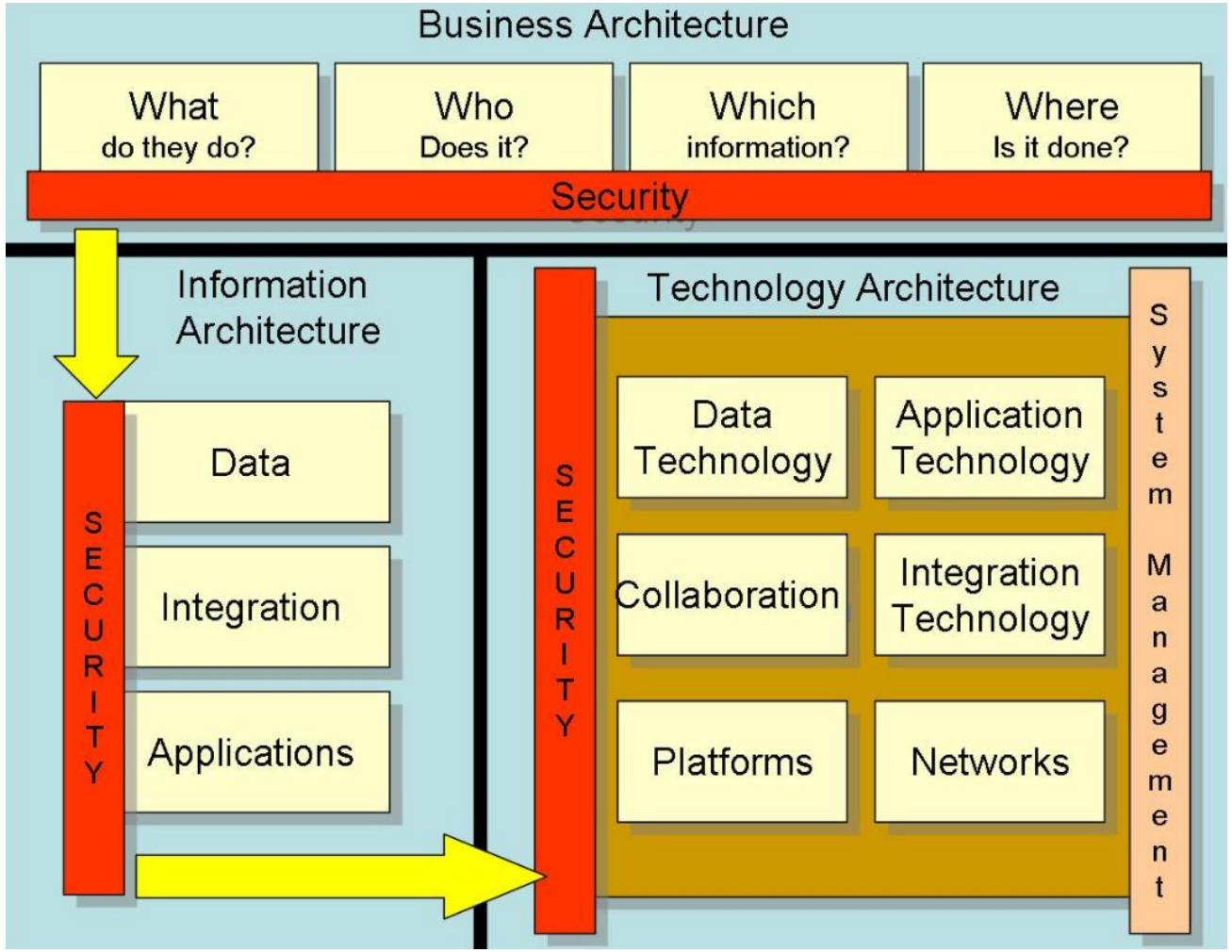
https://graquantum.com/blog/cyber-basics-cyber-attack-surface/

Defense in Depth

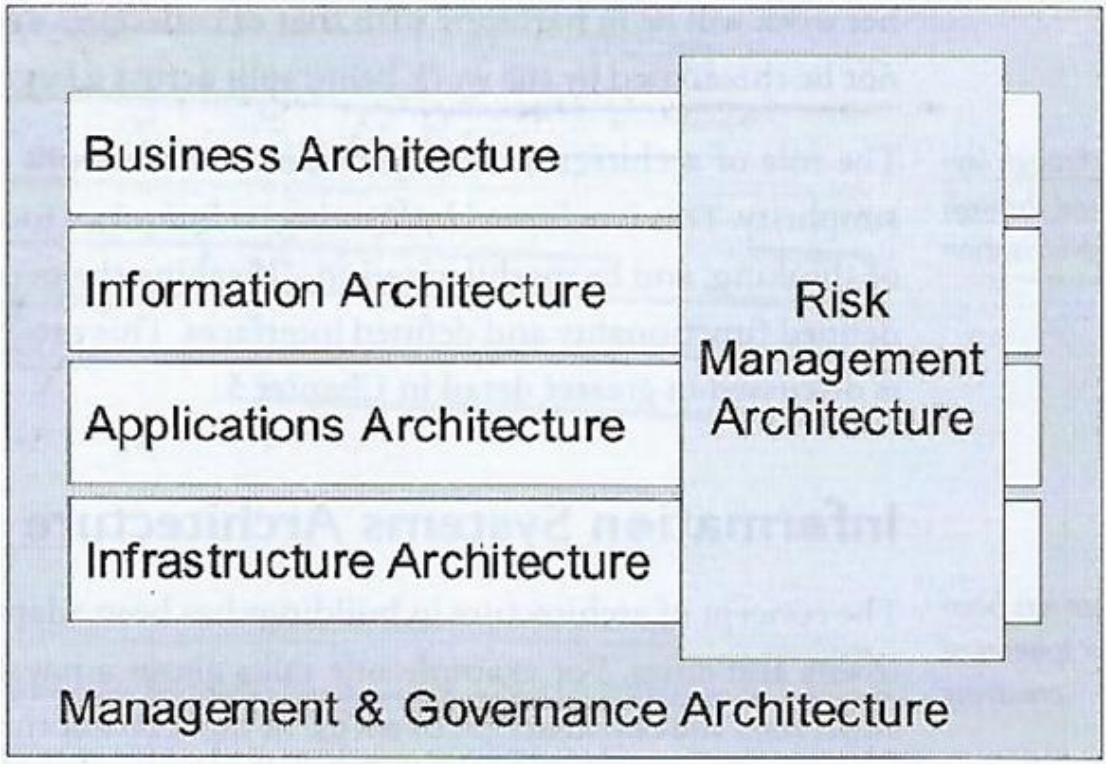
- Also known as:
  - Layered security
  - “Castle” approach to security



Enterprise Information and Security Architecture



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



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

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

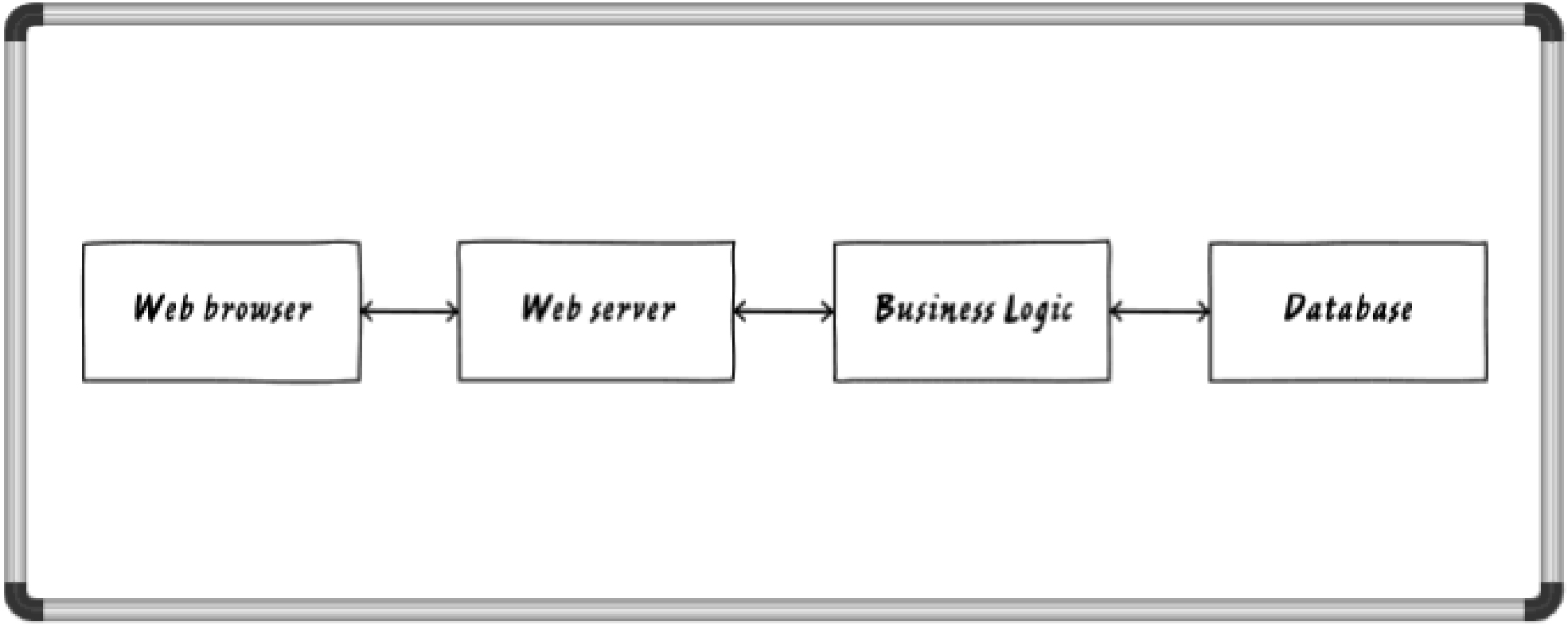
Security architecture framework

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 or has been built?

- Draw a picture of the information system…
- Analyze the picture to see what can go wrong here?

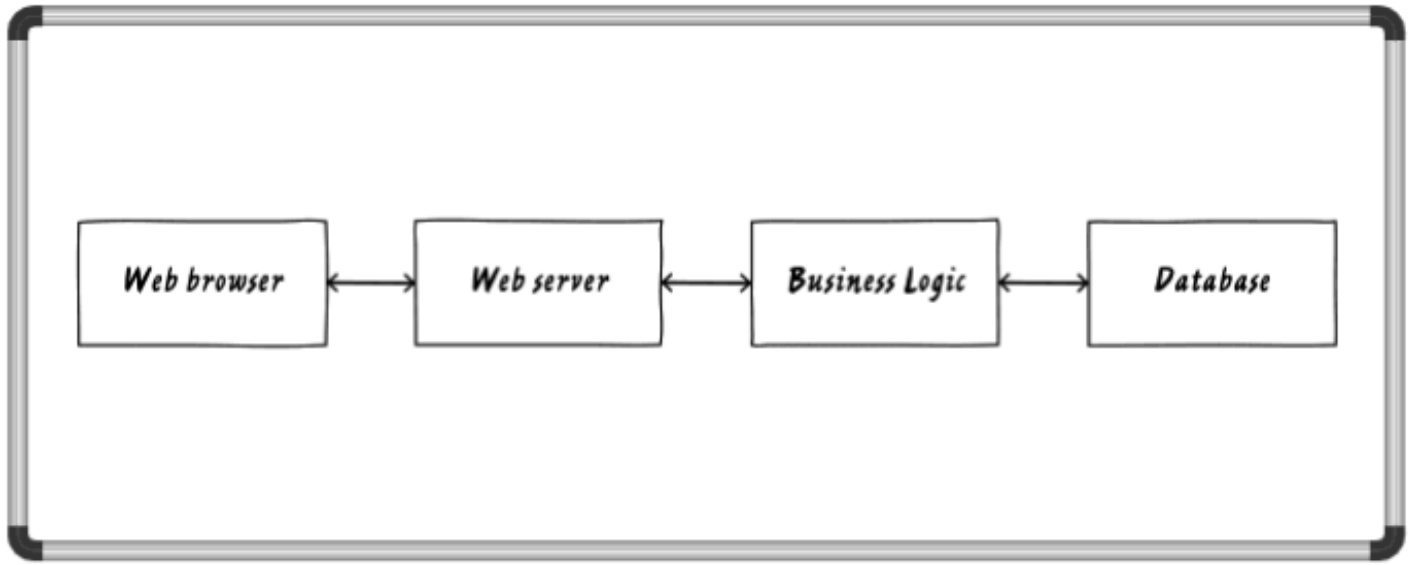


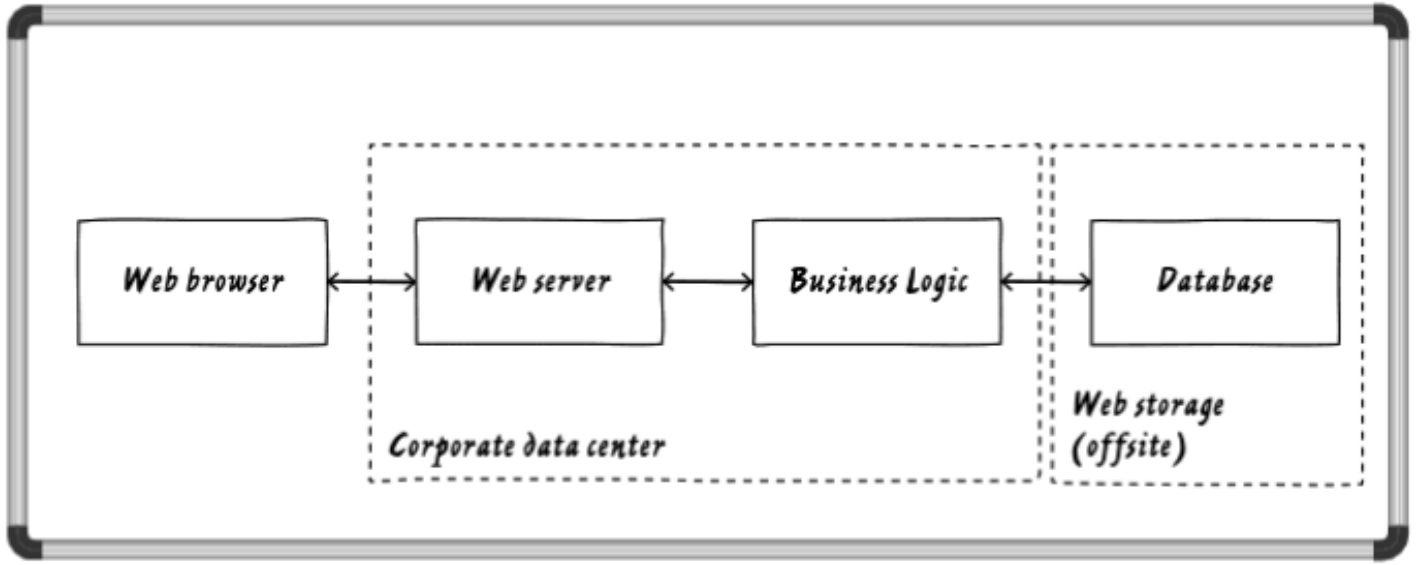
Threat Modeling: Designing for Security, Adam Shostack, 2014

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

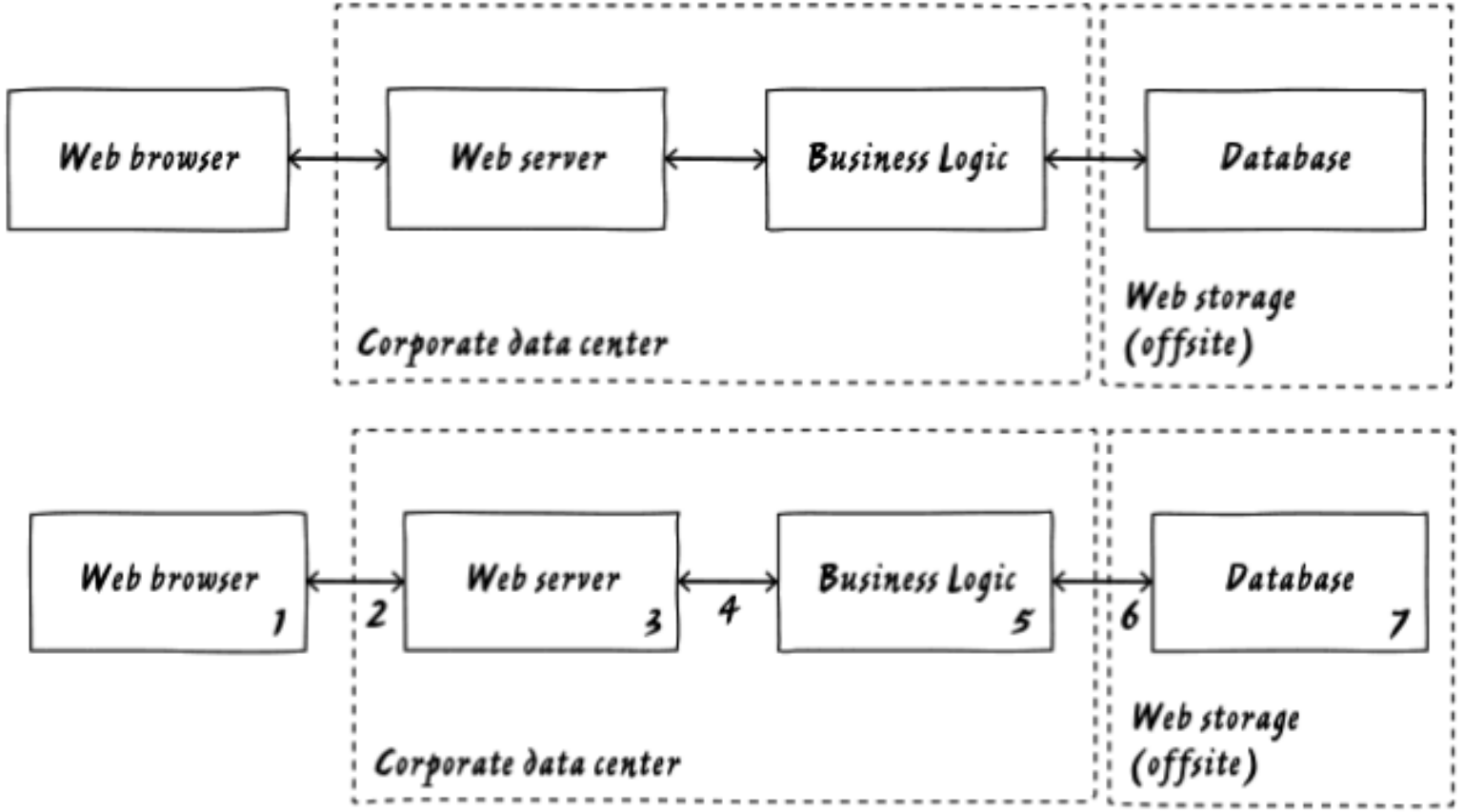
…these are found wherever different people can access and control different parts of the system

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

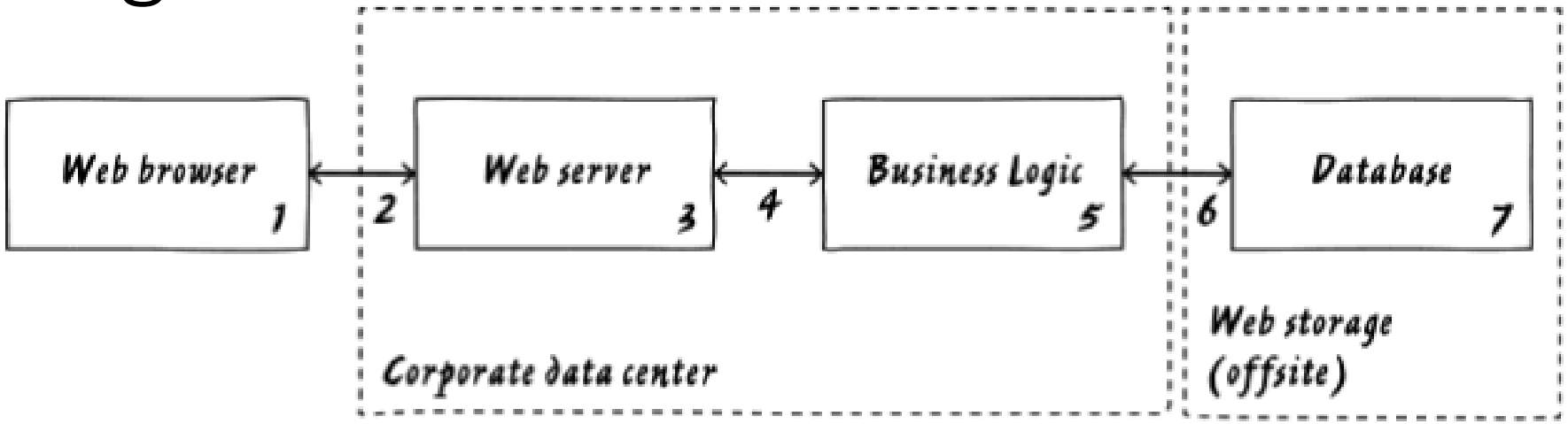




What can go wrong?
Where are the attack surfaces in this system?
Where are the trust boundaries in this system?



What can go wrong?



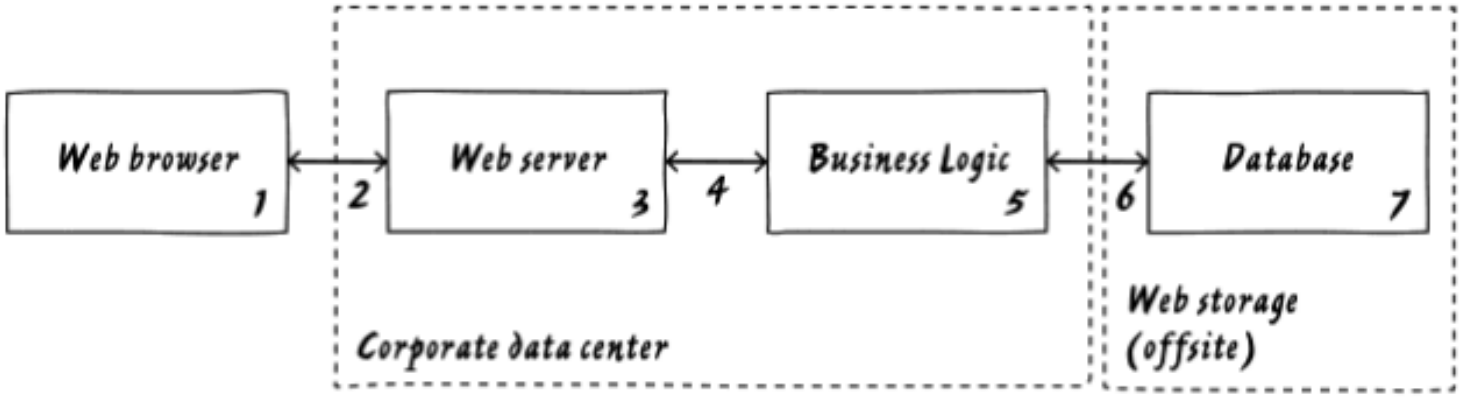
- How do you know the web browser is used by the person you expect?
- Is it OK for data to go from one box to the next without being encrypted?
- What happens if someone made unauthorized modifications to data in the database?

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



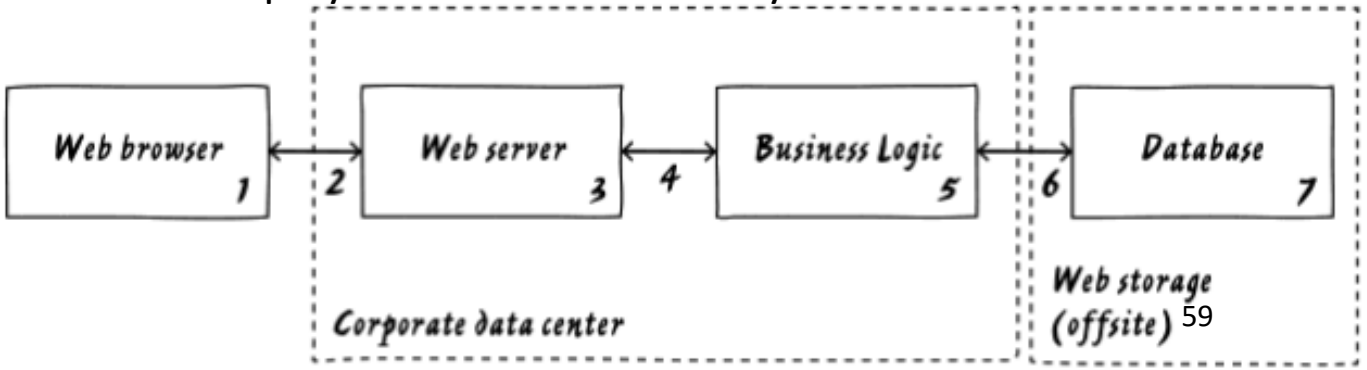
STRIDE

Created by Microsoft to help developers identify threats to security architecture of their systems
Is a mnemonic for 6 categories of threats

- **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, …
- **Elevation of Privileges** …

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?



Techniques for managing threats (i.e. managing risk)

- Avoid
- Accept
- Transfer
- Mitigate

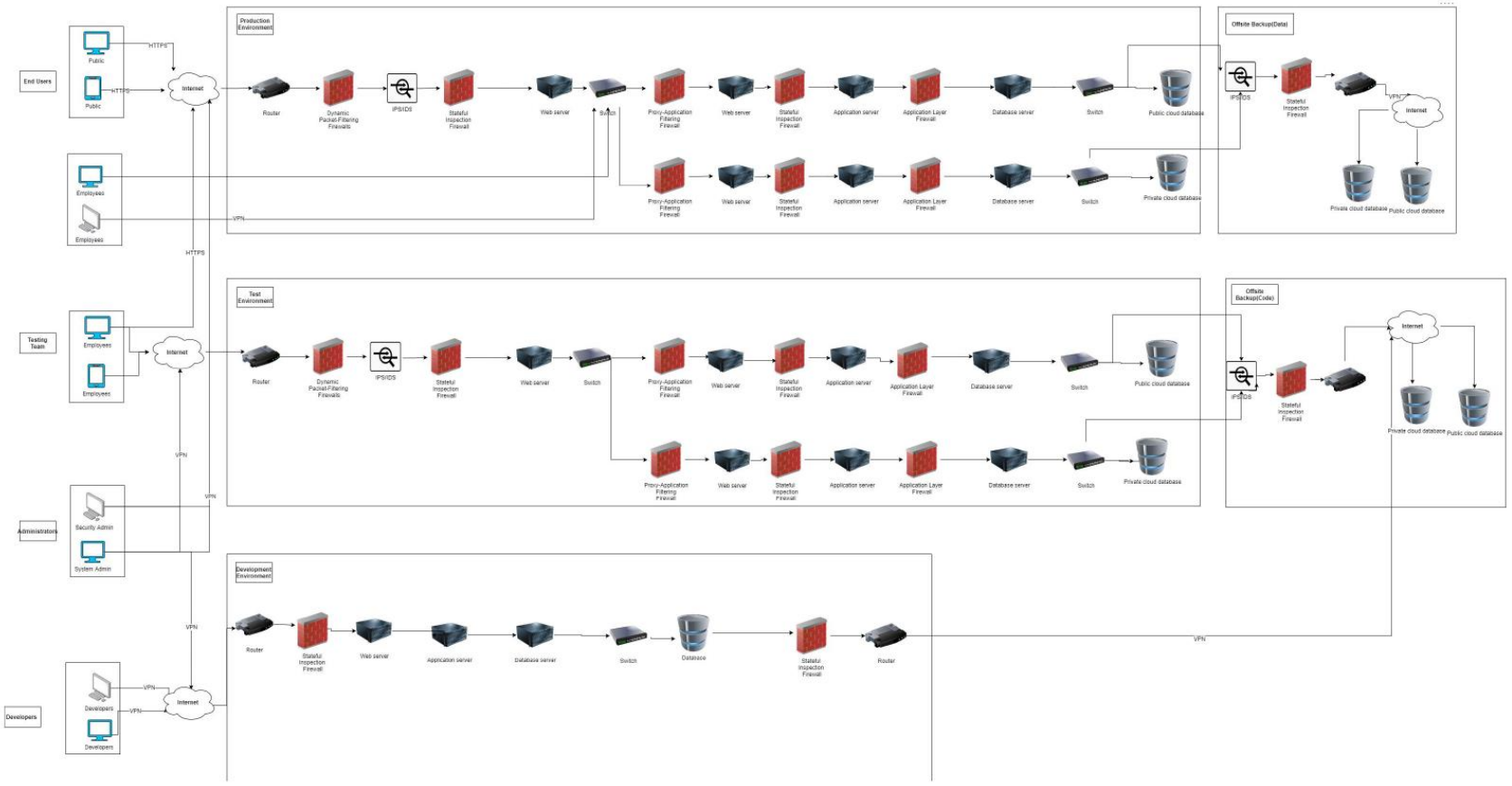
Readings for next week…

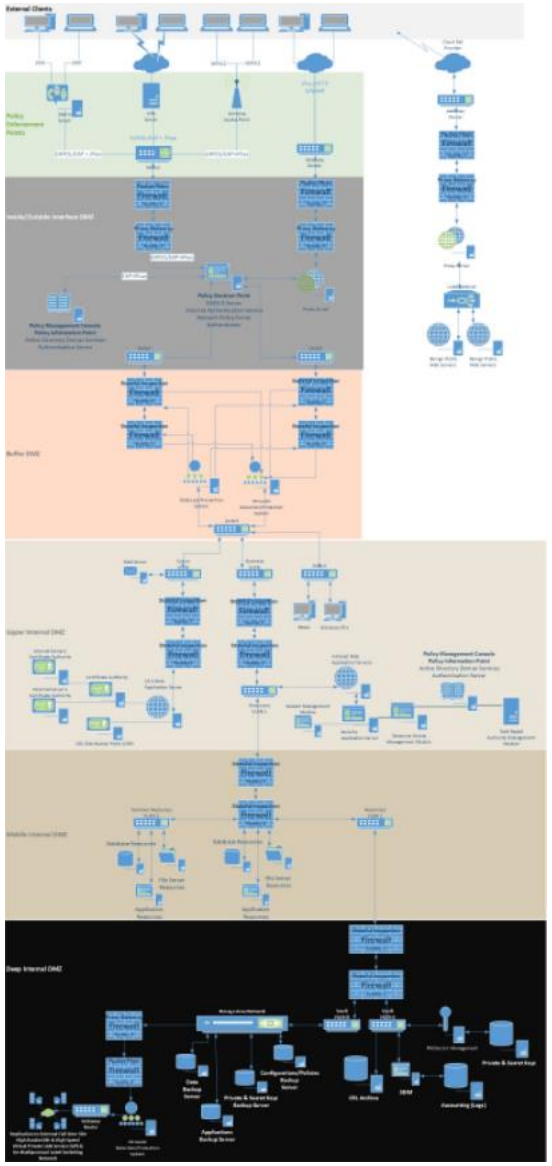
Unit 02 – System Security Plan

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”, pp. 18-26
- “FedRAMP System Security Plan (SSP) High Baseline Template”, Table of Contents and Intro to sections

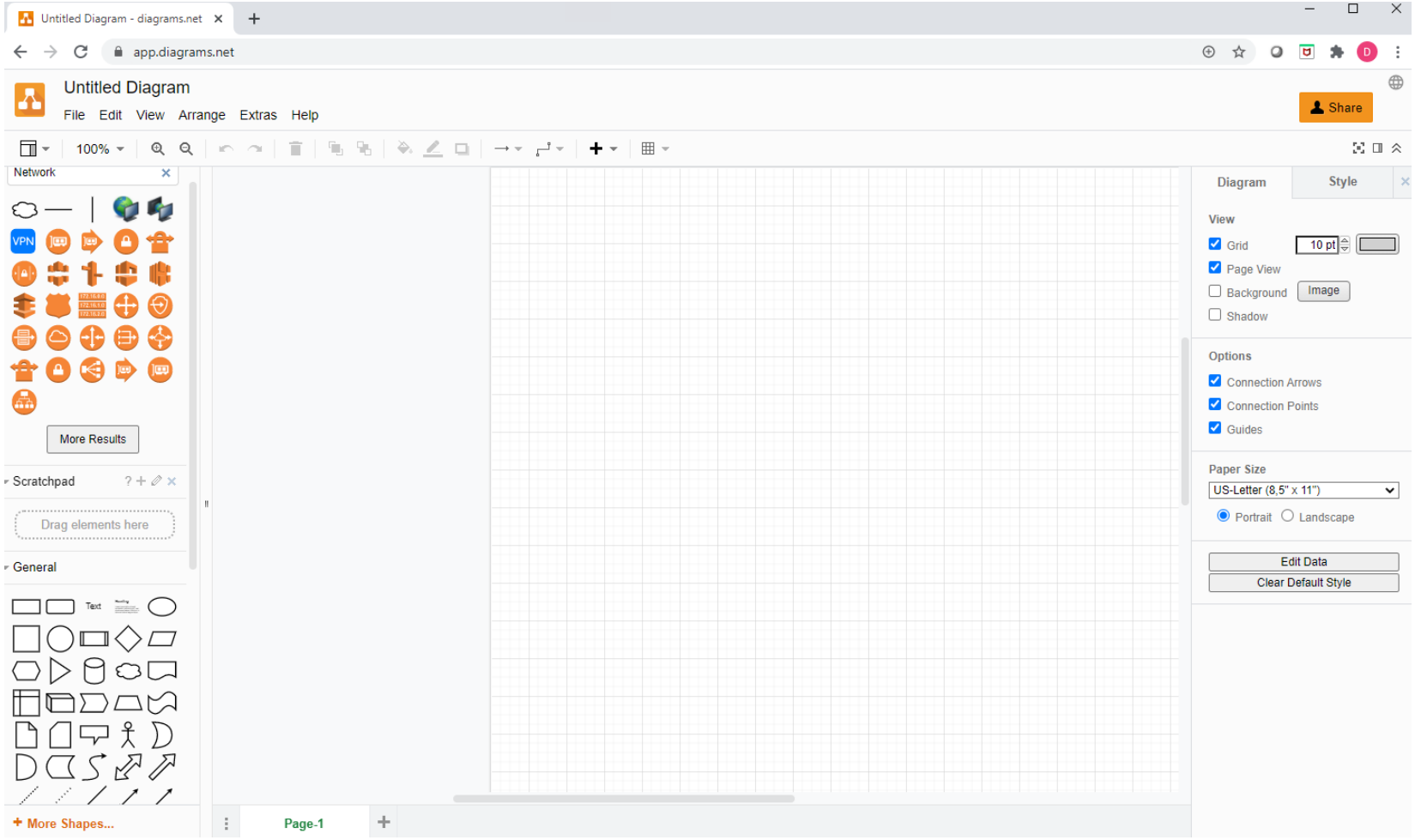
Team Project work involves creating and analyzing security architecture diagrams





Useful tools for the course

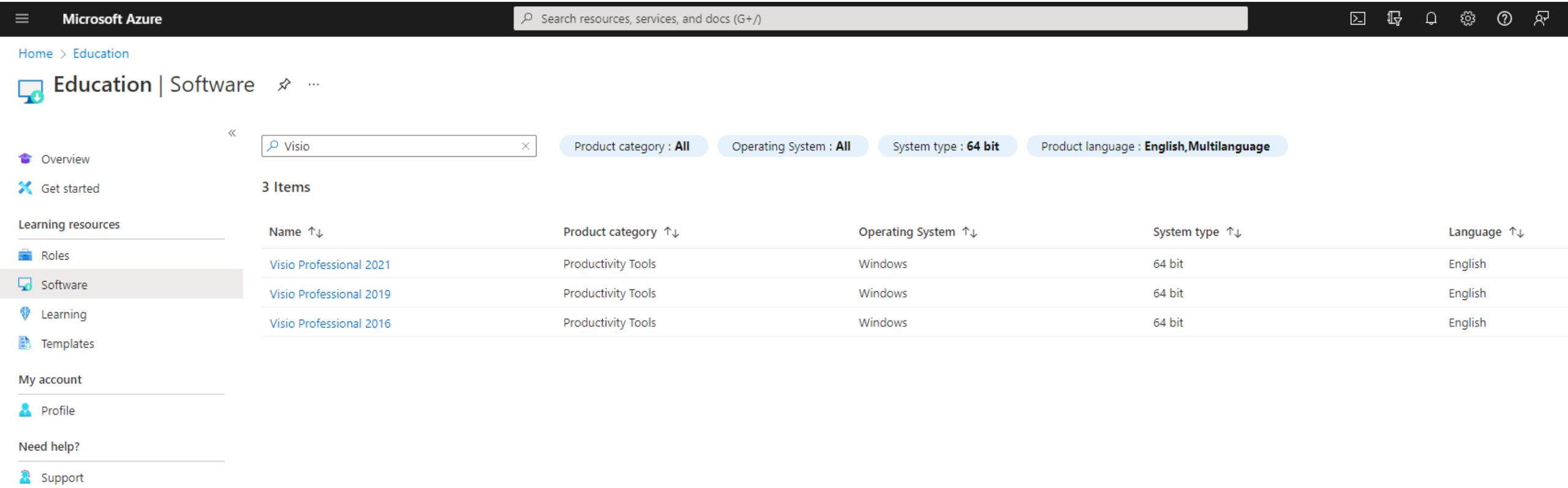
https://app.diagrams.net/



Useful tools for the course

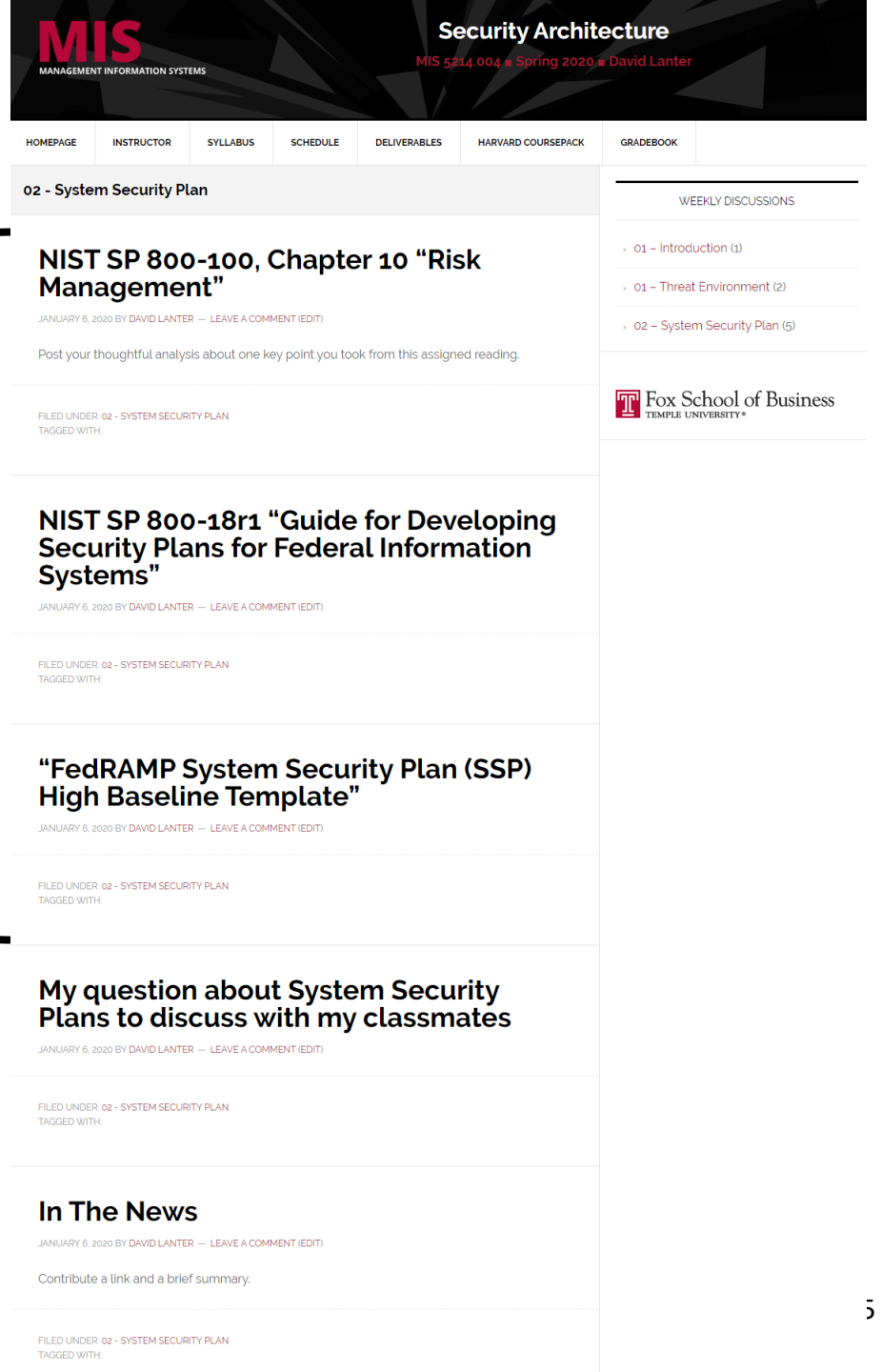
Microsoft Azure education site

https://azureforeducation.microsoft.com/devtools



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