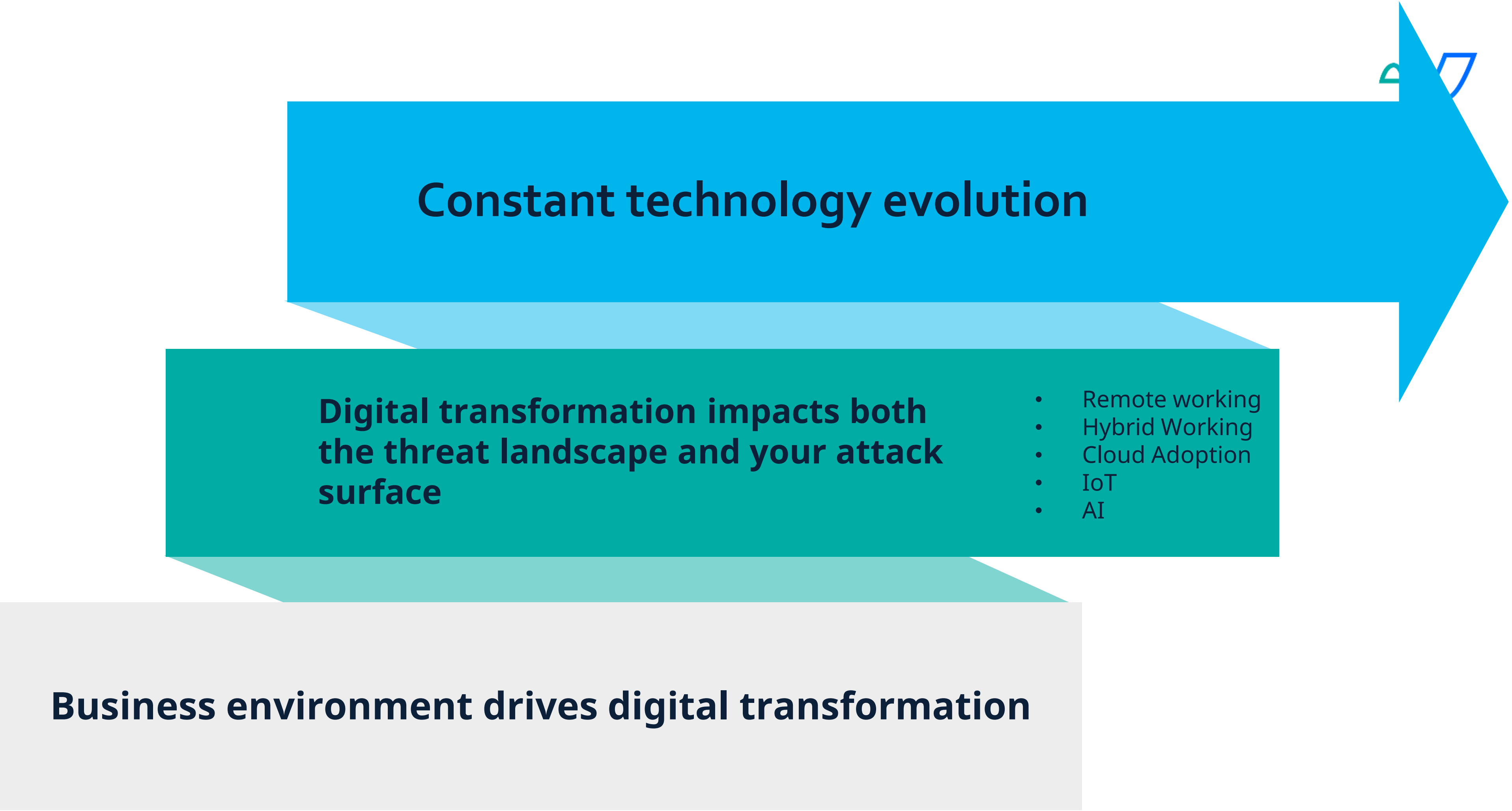
LogRhythm®

Current Cybersecurity Landscape

Andrew Hollister, CISO

13 September 2023

Current Business Environment



Constant technology evolution

Digital transformation impacts both the threat landscape and your attack surface

- Remote working
- Hybrid Working
- Cloud Adoption
- IoT
- AI

Business environment drives digital transformation

Threat Landscape Research

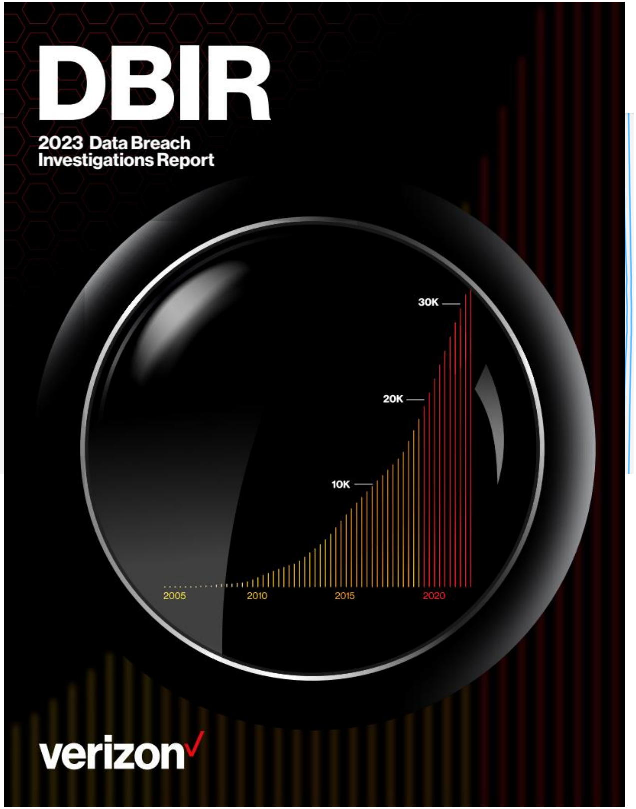
enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT
LANDSCAPE 2022

(July 2021 to July 2022)

OCTOBER 2021



DBIR

2023 Data Breach
Investigations Report

verizon

http://verizon.com/dbir/

CROWDSTRIKE

2023
GLOBAL
THREAT
REPORT

Verizon DBIR 2023

- **16,312 Incidents**
- **5,199 Breaches**

- **Incident**: A security event that compromises the integrity, confidentiality or availability of an information asset.

- **Breach**: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

  A Distributed Denial of Service (DDoS) attack, for instance, is most often an incident rather than a breach, since no data is exfiltrated. That doesn't make it any less serious.

Source: "Verizon 2023 Data Breach Investigations Report"

Success is stumbling from failure to failure with no loss of enthusiasm

Sir Winston Churchill

DBIR – Some key findings

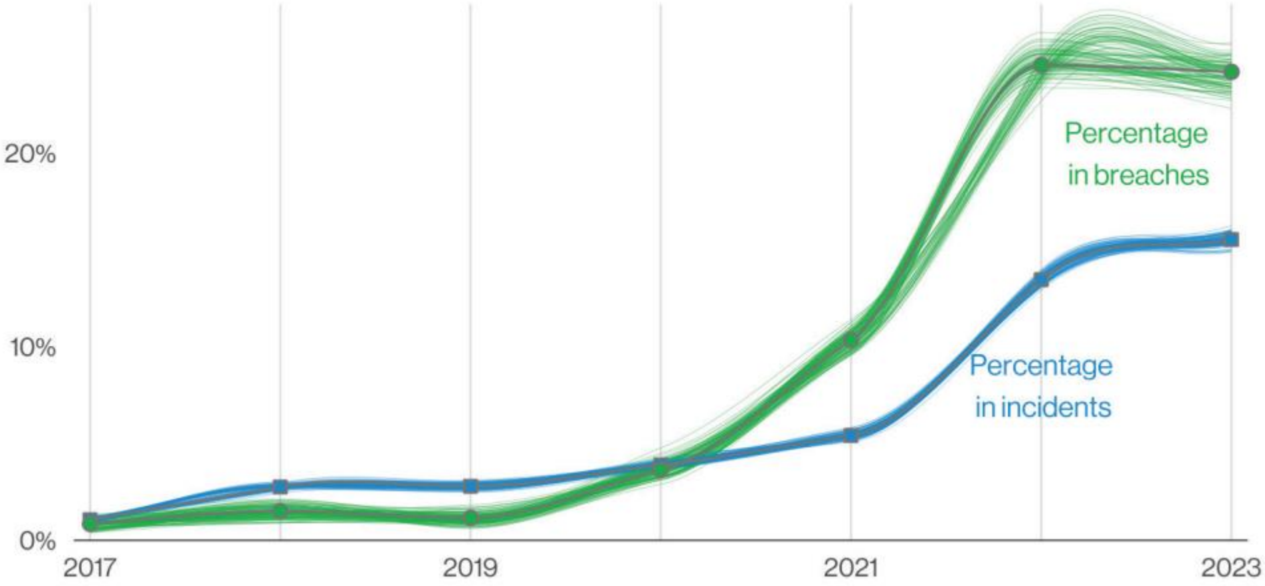


Figure 4. Ransomware action variety over time

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

Source: “Verizon 2023 Data Breach Investigations Report”

DBIR – Some key findings

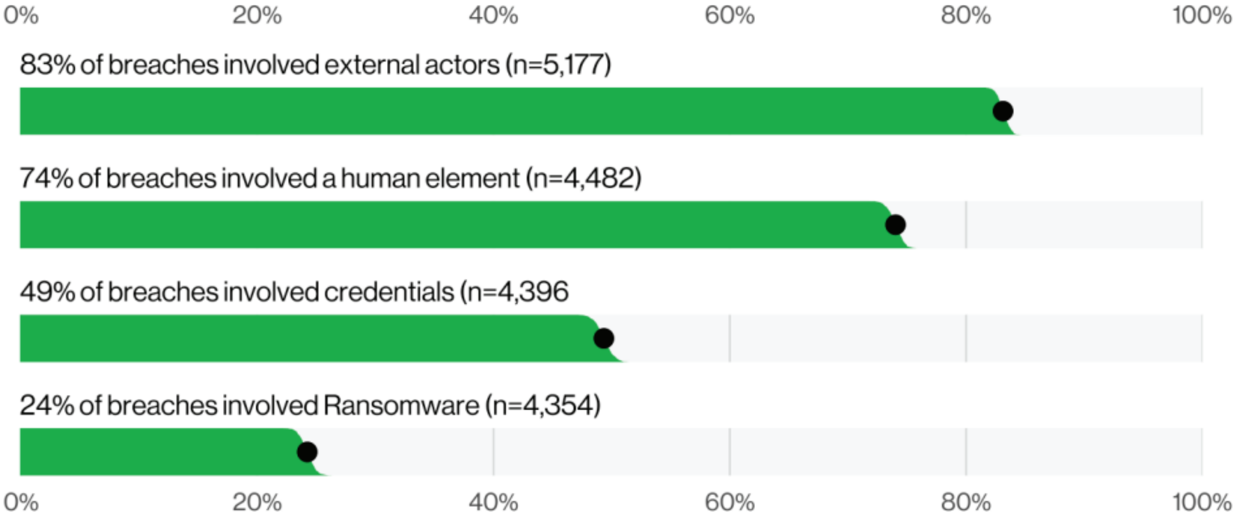


Figure 5. Select key enumerations

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

Source: "Verizon 2023 Data Breach Investigations Report"

DBIR – Some key findings

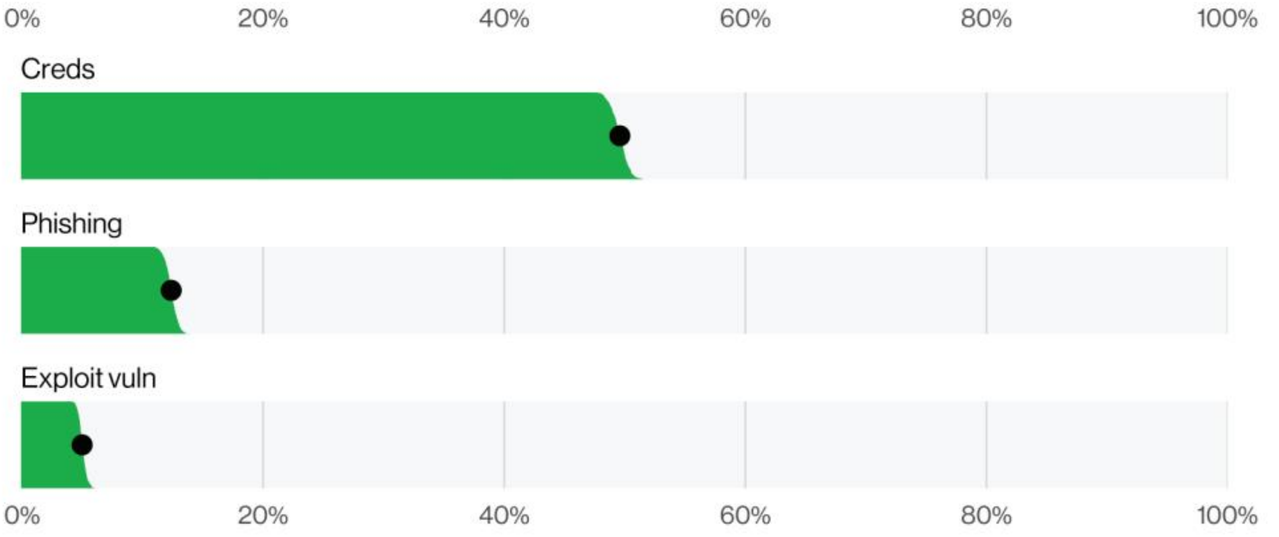
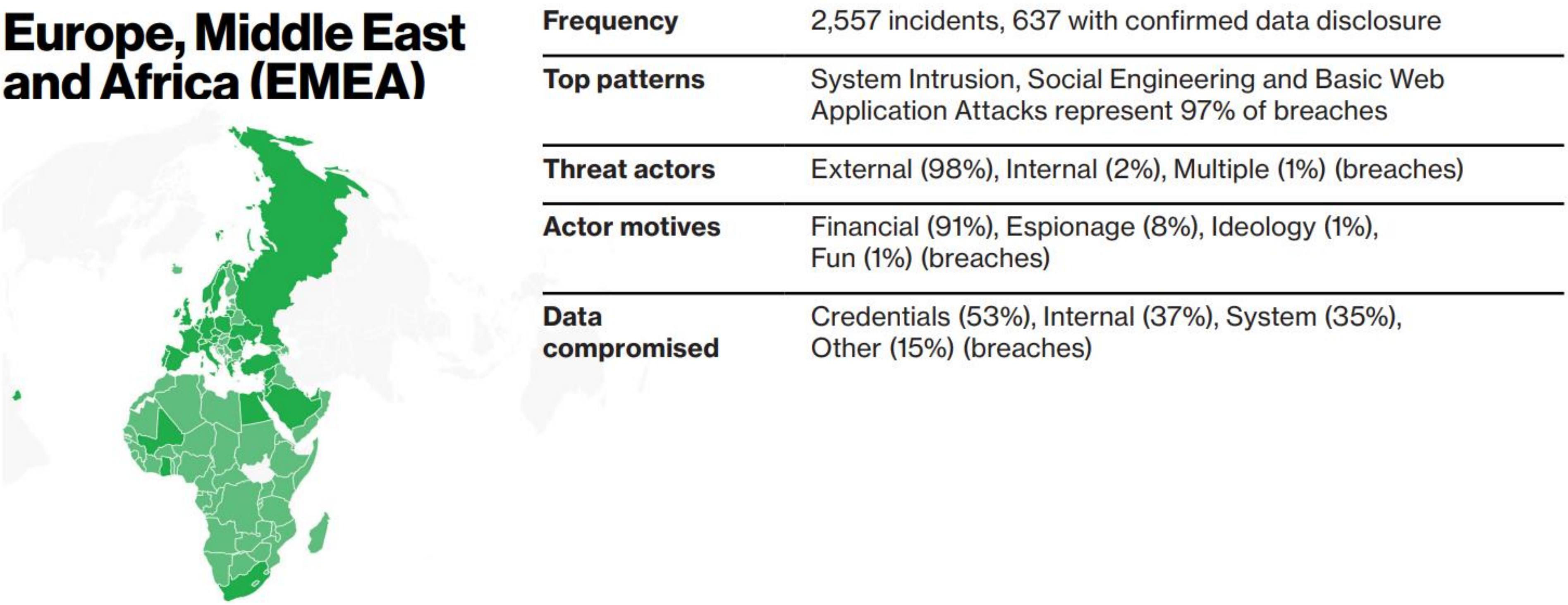


Figure 6. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Source: “Verizon 2023 Data Breach Investigations Report”

DBIR – Some key findings



Europe, Middle East and Africa (EMEA)

Frequency	2,557 incidents, 637 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches
Threat actors	External (98%), Internal (2%), Multiple (1%) (breaches)
Actor motives	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)
Data compromised	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)

Source: “Verizon 2023 Data Breach Investigations Report”

Neuberger: Ukraine experiencing a ‘surge’ in cyberattacks as it executes counteroffensive

UK universities at high risk of major cyberattacks

NSA warns of ‘false sense of security’ against BlackLotus malware

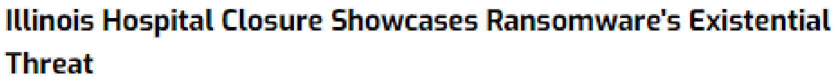
Ransomware attacks pose communications dilemmas for local governments

China-sponsored APT group targets government ministries in the Americas

Largest public pension fund in US affected by MOVEit breach

Attackers set up rogue GitHub repos with malware posing as zero-day exploits

British law firms warned to upgrade cyberdefenses against ransomware attacks



Illinois Hospital Closure Showcases Ransomware's Existential Threat

Companies and Governments Disclose Data Theft From Attack on File-Sharing Tool

Food Producers Band Together in Face of Cyber Threats

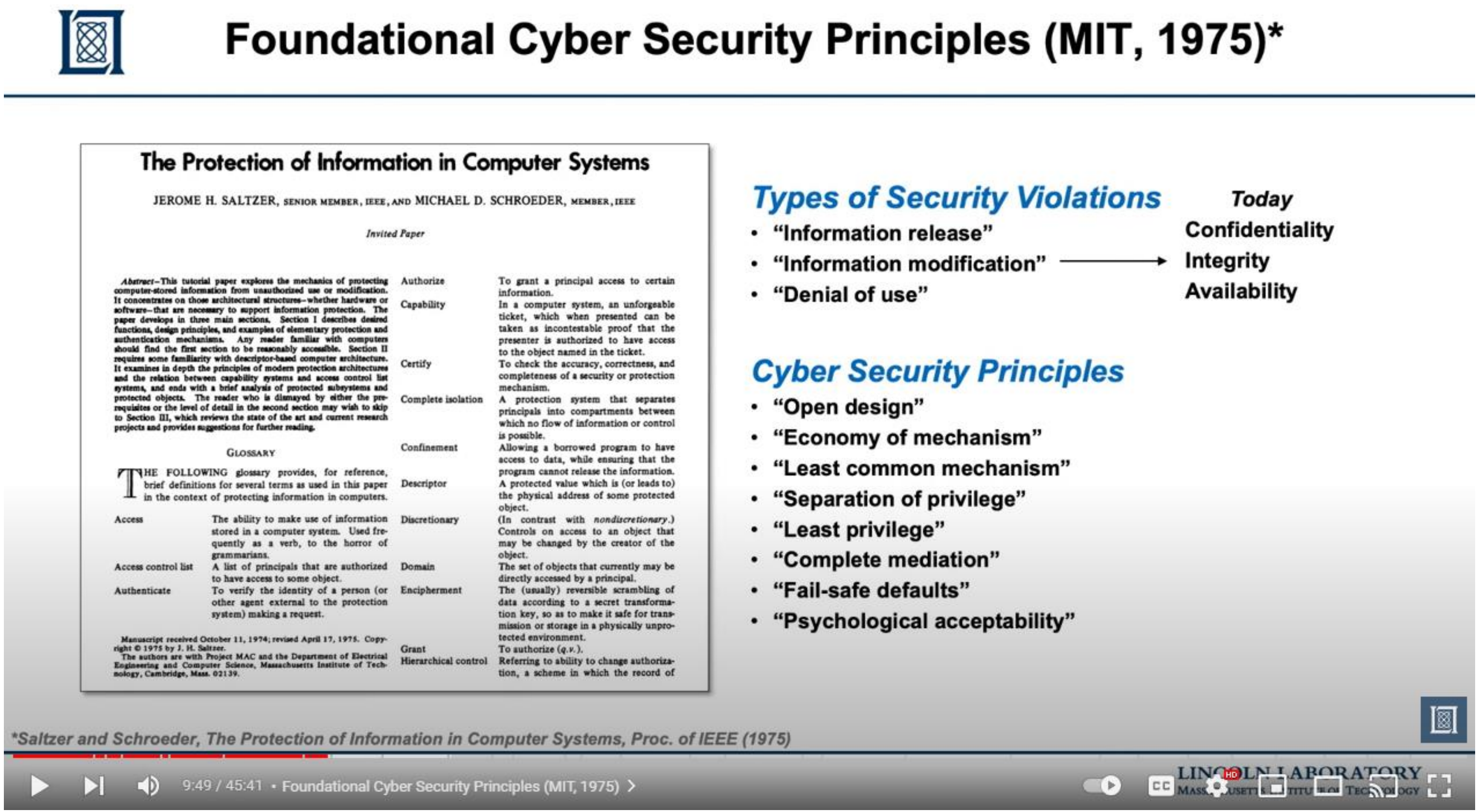
Council contacts 7,000 after data hack

USB Drives Spread Spyware as China's Mustang Panda APT Goes Global

Cyberattacks on OT, ICS Lay Groundwork for Kinetic Warfare

What is “Cybersecurity”?

Overview of Zero Trust Architectures – MIT Lincoln Lab



Foundational Cyber Security Principles (MIT, 1975)*

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

Invited Paper

Abstract–This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures–whether hardware or software–that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with descriptor-based computer architecture. It examines in depth the principles of modern protection architectures and the relation between capability systems and access control list systems, and ends with a brief analysis of protected subsystems and protected objects. The reader who is dismayed by either the prerequisites or the level of detail in the second section may wish to skip to Section III, which reviews the state of the art and current research projects and provides suggestions for further reading.

GLOSSARY

THE FOLLOWING glossary provides, for reference, brief definitions for several terms as used in this paper in the context of protecting information in computers.

Access — The ability to make use of information stored in a computer system. Used frequently as a verb, to the horror of grammarians.

Access control list — A list of principals that are authorized to have access to some object.

Authenticate — To verify the identity of a person (or other agent external to the protection system) making a request.

Authorize — To grant a principal access to certain information.

Capability — In a computer system, an unforgeable ticket, which when presented can be taken as incontestable proof that the presenter is authorized to have access to the object named in the ticket.

Certify — To check the accuracy, correctness, and completeness of a security or protection mechanism.

Complete isolation — A protection system that separates principals into compartments between which no flow of information or control is possible.

Confinement — Allowing a borrowed program to have access to data, while ensuring that the program cannot release the information.

Descriptor — A protected value which is (or leads to) the physical address of some protected object.

Discretionary — (In contrast with *nondiscretionary*.) Controls on access to an object that may be changed by the creator of the object.

Domain — The set of objects that currently may be directly accessed by a principal.

Encipherment — The (usually) reversible scrambling of data according to a secret transformation key, so as to make it safe for transmission or storage in a physically unprotected environment.

Grant — To authorize (*q.v.*).

Hierarchical control — Referring to ability to change authorization, a scheme in which the record of

Manuscript received October 11, 1974; revised April 17, 1975. Copyright © 1975 by J. H. Saltzer.

The authors are with Project MAC and the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, Mass. 02139.

Types of Security Violations

- "Information release"
- "Information modification" →
- "Denial of use"

Today

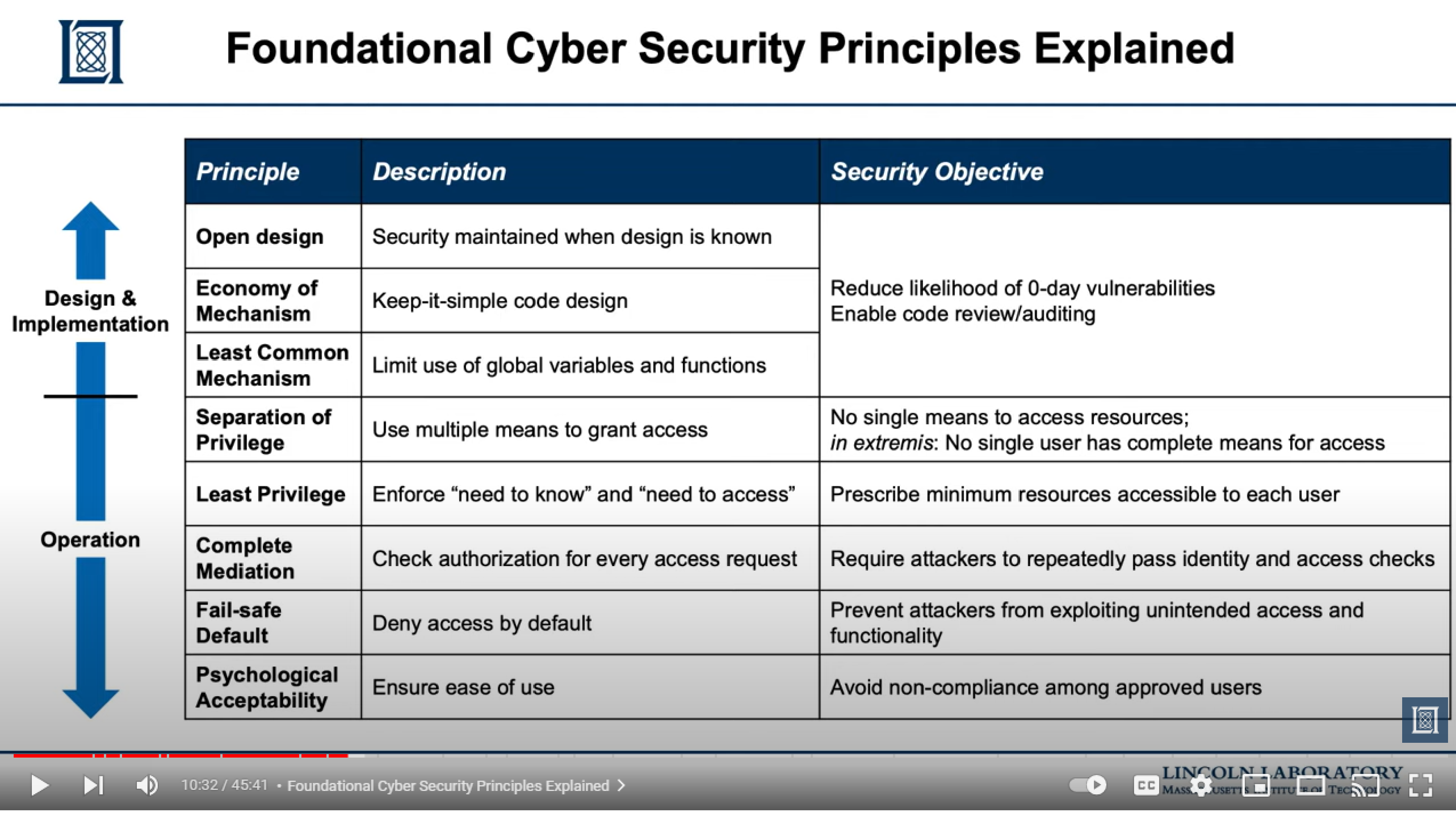
Confidentiality
Integrity
Availability

Cyber Security Principles

- "Open design"
- "Economy of mechanism"
- "Least common mechanism"
- "Separation of privilege"
- "Least privilege"
- "Complete mediation"
- "Fail-safe defaults"
- "Psychological acceptability"

*Saltzer and Schroeder, The Protection of Information in Computer Systems, Proc. of IEEE (1975)

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
9:49 / 45:41 • Foundational Cyber Security Principles (MIT, 1975) ›
HD
CC



Foundational Cyber Security Principles Explained

Design & Implementation

Operation

Principle	*Description*	*Security Objective*
Open design	Security maintained when design is known	Reduce likelihood of 0-day vulnerabilities Enable code review/auditing
Economy of Mechanism	Keep-it-simple code design	
Least Common Mechanism	Limit use of global variables and functions	
Separation of Privilege	Use multiple means to grant access	No single means to access resources; *in extremis*: No single user has complete means for access
Least Privilege	Enforce “need to know” and “need to access”	Prescribe minimum resources accessible to each user
Complete Mediation	Check authorization for every access request	Require attackers to repeatedly pass identity and access checks
Fail-safe Default	Deny access by default	Prevent attackers from exploiting unintended access and functionality
Psychological Acceptability	Ensure ease of use	Avoid non-compliance among approved users

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

10:32 / 45:41 • Foundational Cyber Security Principles Explained ›

The Process of Security

- If we’ve learned anything from the past couple of years, it’s that computer security flaws are inevitable. Systems break, vulnerabilities are reported in the press, and still many people put their faith in the next product, or the next upgrade, or the next patch. “This time it’s secure.” So far, it hasn’t been.

Bruce Schneier, April 2000

- **Security is a process, not a product**…. The trick is to reduce your risk of exposure regardless of the products or patches.

- My primary fear about cyberspace is that people don’t understand the risks, and they’re putting too much faith in technology’s ability to obviate them. Products alone can’t solve security problems.

SOAR / Automation

The “Autonomous SOC” Is A Pipe Dream

Allie Mellen, Senior Analyst, Forrester, Oct 26 2022

Manual process automation is limiting because of the following:

- **Like with physical security, humans are still mandatory, even for basic processes.**
- Automation is not designed for complex systems that require resilience.
- Each added step to an automation chain limits the scope of applicability.

Automation built into security technologies is limited because:

- Humans can always outsmart machines.

Avoid threats or Avoid risks?

- Countermeasures are sold as ways to avoid threats.
  - This is completely backwards.

- Security outside of cyber thinks of countermeasures as ways to avoid risk.

- Avoiding threats is black and white; either you avoid the threat, or you don’t.
- Avoiding risk is continuous: there is some amount of risk you can accept, and some amount you can’t.

Bruce Schneier, April 2000

So, what is “Cybersecurity” really?

Cybersecurity is not a project

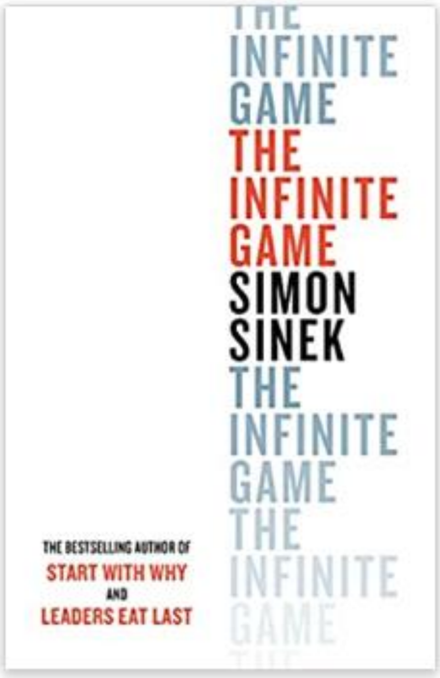
Cybersecurity is not a deterministic state you reach

It’s a persistent cycle of reducing risk

Cybersecurity == continuous improvement.

It’s a never-ending process of surfacing and addressing risk. As the business environment changes over time, so does the digital technology available or in use in your environment. This has a direct impact on the threat landscape, the attack surface of your organisation, and the level of risk.

Success lies not in being 100% secure but in being passionate, courageous, and perseverant to resolve the highest risks in your environment, step by step. You will always have to address security risks - unless you shut down the business!

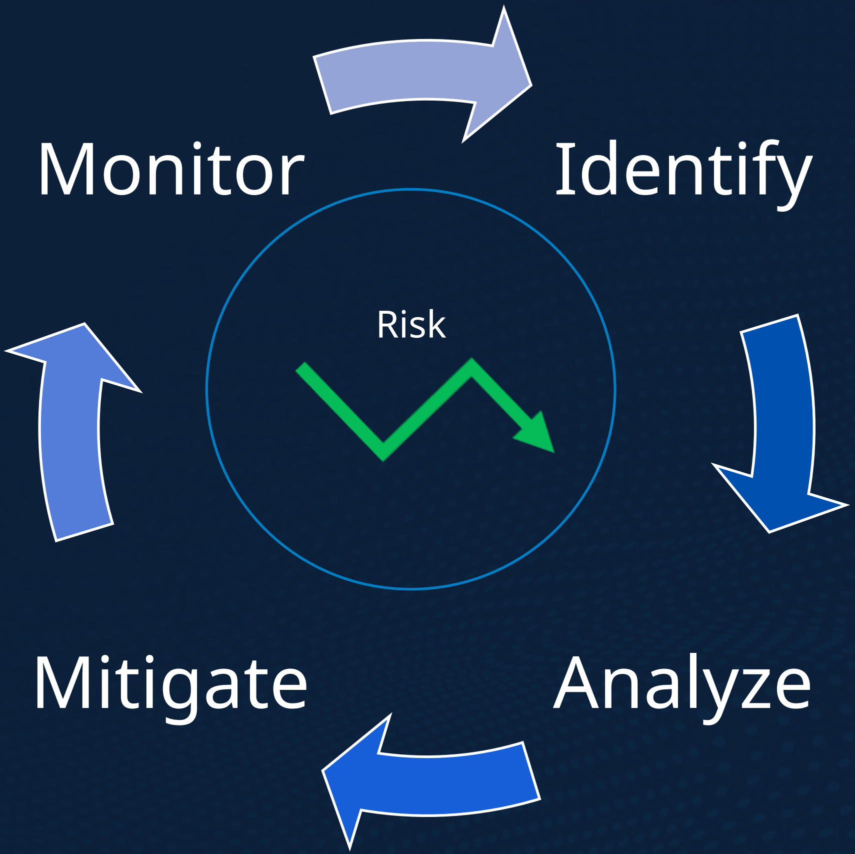


THE
INFINITE
GAME
THE
INFINITE
GAME
SIMON
SINEK
THE
INFINITE
GAME
THE
INFINITE
GAME

THE BESTSELLING AUTHOR OF
START WITH WHY
AND
LEADERS EAT LAST

An infinite game is one with known and unknown players, changeable rules, and no end. The objective is not to win—the objective is to keep playing.

The Cybersecurity Infinite Game


Monitor

Identify

Risk

Analyze

Mitigate

Our Vision and Mission

Ever-evolving digital weaponization is overwhelming security teams despite heroic efforts, making it impossible for them to effectively and efficiently defend against cyberattacks.

Vision

Fast, agile and high-performing security teams armed with the highest-quality signals and automated responses that enable them to confidently defend against digital weaponization.

Mission

To empower security teams with the most intuitive experience and contextual analytics into cybersecurity threats so you can reduce noise, prioritize alerts and quickly secure your environment.

LogRhythm®

- www.youtube.com/user/LogRhythmInc
- www.linkedin.company/logrhythm/
- twitter.com/LogRhythm
- www.facebook.com/LogRhythmInc/