



Threats, Attacks and a Path Forward - 2022

Christopher Rodman – Senior Cybersecurity
Operations Researcher

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notice

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM22-1108

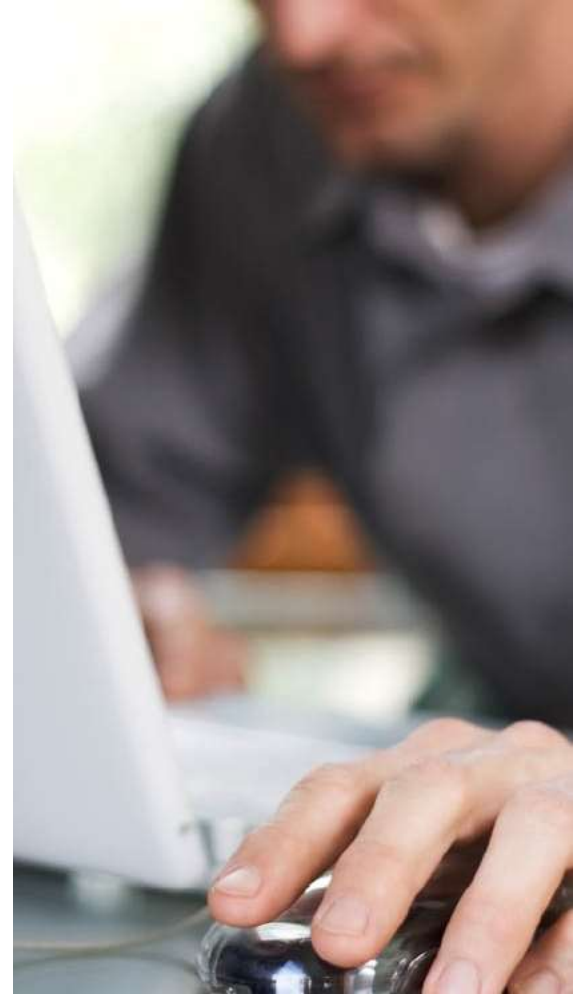
Agenda

Current threats

Attack landscape

The path forward

Current Threats



United States of America: Annual Threat Assessment

Key cybersecurity takeaways from the 2022 Annual Threat Assessment:

- Adversaries remain persistent, advanced and bold in attacks and campaigns
- Key sectors are persistent targets, while motives and methods may vary
 - Critical Infrastructure (Utilities)
 - Transportation
 - Telecommunications/Technology
 - Information (Media and Journalism)
 - Academia
 - Government
 - Defense



Expanded threats with new technologies

Attack surface expansion

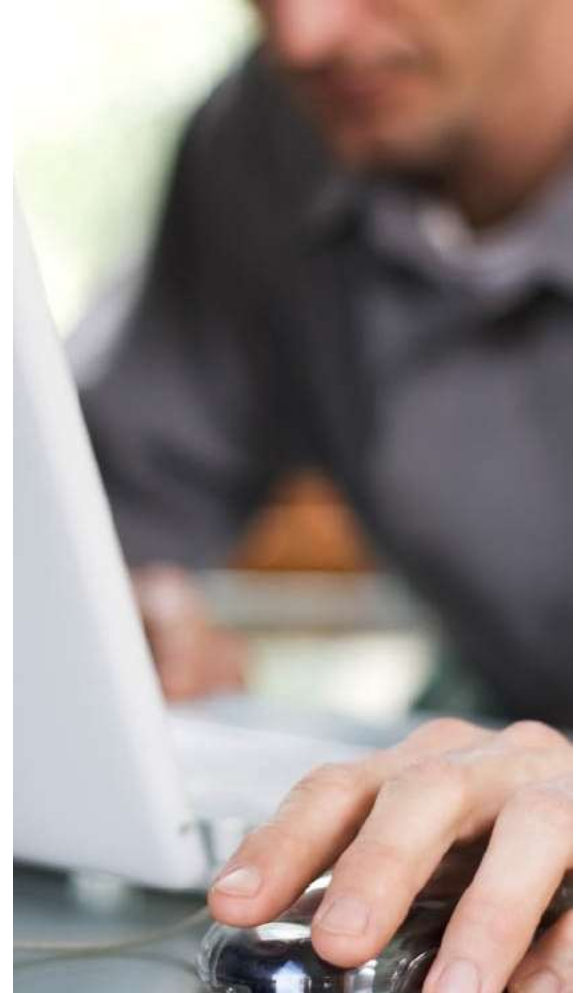
- Remote workforce
- Operational technologies
- Cloud, datacenter and on-premise systems

Identity threat detection and response

- Credential theft
- Credential based attacks

Digital Supply Chain Risk

Attack landscape



Verizon Data Breach Report 2022 by sector

Critical Infrastructure (Utilities)

1. Social Engineering
2. System Intrusion
3. Basic Web Application attacks

Telecommunications/Technology

1. System Intrusion
2. Basic Web application attacks
3. Social Engineering

Information (Media and Journalism)

1. System Intrusion
2. Basic Web Application attacks
3. Miscellaneous errors

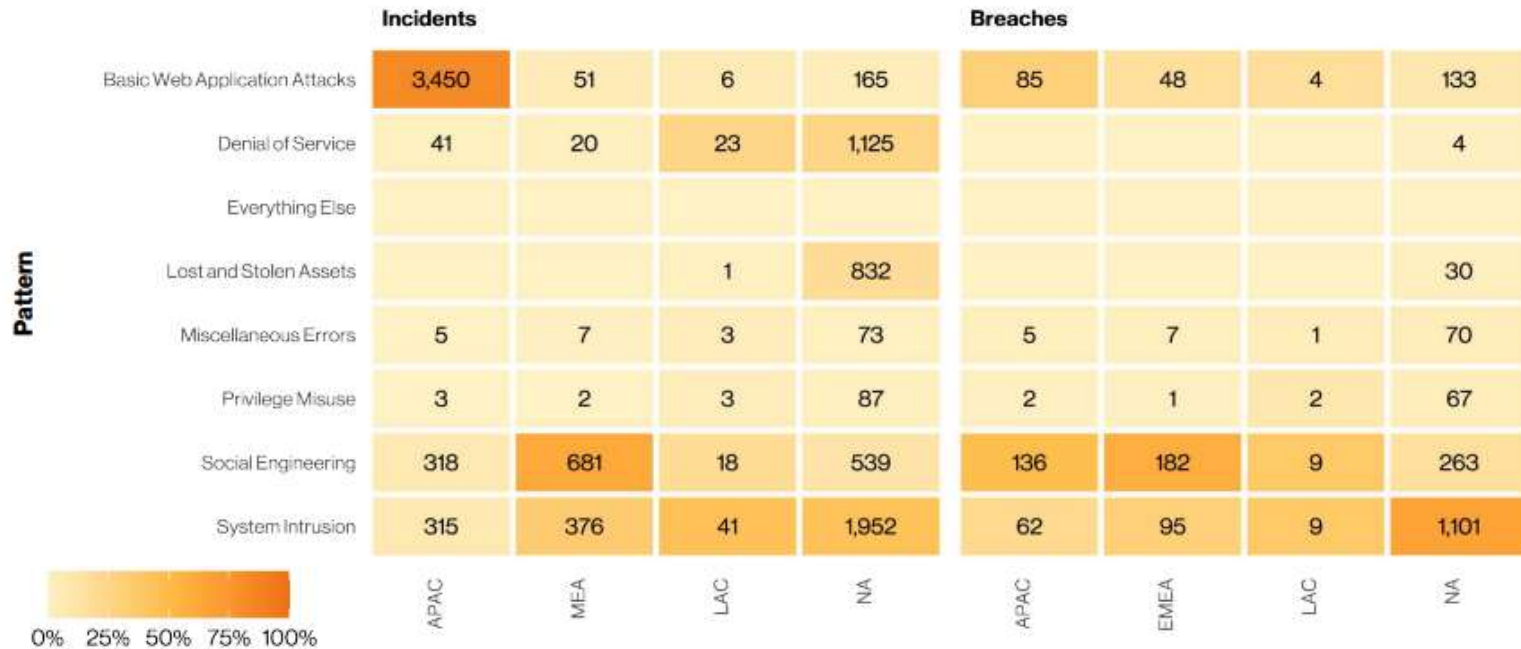
Academia

1. System Intrusion
2. Basic Web Application attacks
3. Miscellaneous errors

Government

1. System Intrusion
2. Miscellaneous errors
3. Basic Web Application attacks

Verizon Data Breach Report 2022 by region



Source: Verizon.com

But what about...

Ransomware...

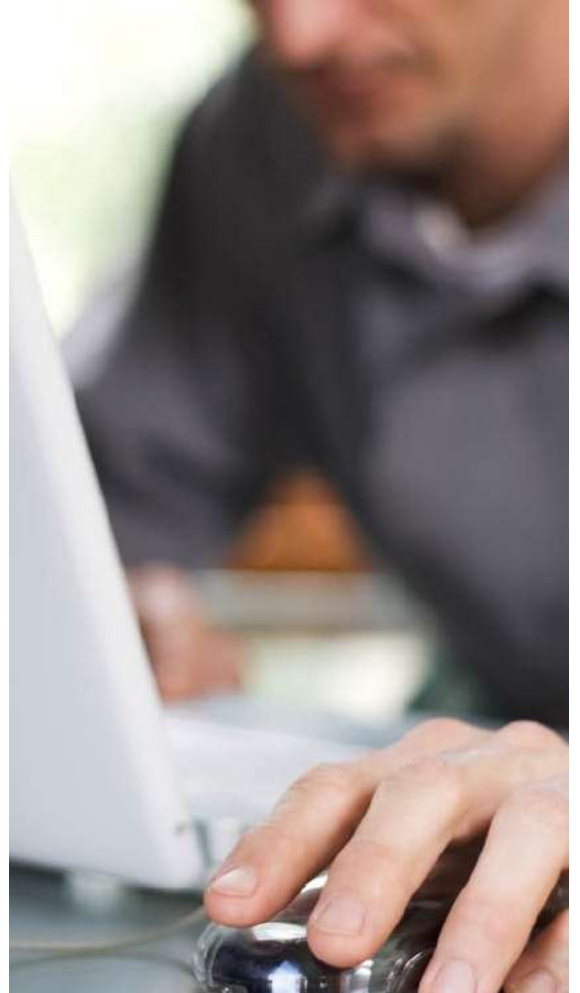
Supply chain attacks...

Cryptocurrency...

Internet of Things...

And so on...

The path forward



Security controls that apply

Center for Internet Security (CIS) Critical Controls

- Access Control Management
- Account Management
- Secure Configuration of Enterprise Assets and Software
- Security Awareness and Skills Training



Source: [cisecurity.org](https://www.cisecurity.org)

Looking into the future

New products and services may ease implementation of security measures

Technology shifts

- Vendor consolidation
- Cybersecurity mesh

Changes of practice

- Culture of security
- Risk decision distribution



Source: *keyfactor.com*

If you would like to know more

<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf>

<https://www.verizon.com/business/resources/T1d7/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>

<https://www.cisecurity.org/>

<https://www.keyfactor.com/blog/what-you-need-to-know-about-cybersecurity-mesh/>