SecureFi Institute
An OnShoreWave Business

COURSE 3 PROFESSIONAL REFERENCE

Real-World Trust Failures

Use Cases from Cyber-Ready Trusted Systems Engineering

Modern systems fail when trusted relationships are assumed rather than continuously verified. These 14 incidents show how attackers and insiders exploited firmware, identity, vendors, applications, recovery paths, and governance gaps.

How to use this reference

Use each case to identify the trust relationship that failed, the control that was assumed, and the evidence your organization would need to confirm that the same exposure does not exist in its own environment.

- Ask where your organization relies on identity, software provenance, vendor access, or internal network trust without independent verification.
- Identify which team owns the control, which evidence proves it is operating, and how quickly the organization would detect a failure.
- Translate the lesson into a named action, accountable owner, and target date for the 90-day Trusted Systems roadmap.

The cases at a glance

Trust theme	Cases included
Platform Origin and Software Integrity	MoonBounce / APT41 • DigiNotar • SolarWinds SUNBURST
Identity Privilege and Human Trust	Midnight Blizzard / Microsoft • Lapsus$ / Okta-Sitel • Jack Teixeira • Samsung / ChatGPT
Applications Vendors and Long-Lived Data	MOVEit / Cl0p • Equifax • OPM Background Investigation Breach
Infrastructure Resilience and Recovery	NotPetya / Maersk • Triton / TRISIS • Maersk Recovery / Ghana AD • Volt Typhoon

SecureFi Institute
An OnShoreWave Business

TRUSTED SYSTEMS CASE SERIES

Platform Origin and Software Integrity

Trust can be compromised before software or a system reaches the user. These cases show how firmware, certificate authorities, and build pipelines can turn trusted components into durable attack paths.

MoonBounce / APT41 2022

What happened	How trust was exploited
UEFI firmware implant discovered in motherboard SPI flash, allowing persistence below the operating system.	Initial intrusion path was not publicly established. After privileged access was obtained, the adversary implanted firmware-level persistence that could survive OS reinstall and disk replacement.

DigiNotar 2011

What happened	How trust was exploited
A trusted Dutch certificate authority was compromised and fraudulent certificates, including for Google, were issued.	The attacker compromised the CA infrastructure and weaponized the existing browser trust model. Rogue certificates could impersonate legitimate services and enable interception.

SolarWinds SUNBURST 2019-2020

What happened	How trust was exploited
Attackers compromised the SolarWinds Orion build process and distributed malicious, legitimately signed software.	The build environment itself was compromised, allowing SUNBURST to be inserted before legitimate signing and distribution. Customers trusted the vendor, signature, and update channel.

SecureFi Institute
An OnShoreWave Business

TRUSTED SYSTEMS CASE SERIES

Identity Privilege and Human Trust

Legitimate identities and authorized relationships can become the intrusion path. These cases show why access must be bounded, monitored, and aligned to purpose.

Midnight Blizzard / Microsoft 2024

What happened	How trust was exploited
Russian state-linked actor accessed Microsoft corporate email through identity and OAuth abuse.	Password spraying compromised a legacy non-production account without MFA. The actor then abused OAuth applications and powerful Exchange application permissions to reach targeted mailboxes.

Lapsus$ / Okta-Sitel 2022

What happened	How trust was exploited
A third-party support environment connected to Okta was compromised.	The attacker compromised a Sitel support engineer workstation and used the legitimate support relationship and administrative access available through that endpoint.

Jack Teixeira 2022-2023

What happened	How trust was exploited
Classified intelligence was disclosed to an online Discord community.	This was an insider-trust failure, not an external intrusion. Teixeira had legitimate access to classified systems but accessed material beyond his assigned duties and disclosed it through physical and online means.

Samsung / ChatGPT March 2023

What happened	How trust was exploited
Employees submitted proprietary semiconductor code and confidential information to ChatGPT in several incidents.	No external attacker broke in. Sensitive information crossed the organizational trust boundary because employees placed proprietary data into an externally hosted AI service without sufficient governance.

TRUSTED SYSTEMS CASE SERIES

Applications Vendors and Long-Lived Data

Application weaknesses and third-party platforms can expose data at scale. These cases show how a single unverified dependency can expand risk across organizations and over time.

MOVEit / Cl0p 2023

What happened	How trust was exploited
A zero-day in MOVEit Transfer enabled mass theft of files across thousands of downstream organizations.	Cl0p exploited an unauthenticated SQL-injection vulnerability in a trusted file-transfer platform, gaining application-level access to stored customer data without first compromising each customer separately.

Equifax 2017

What happened	How trust was exploited
Attackers exploited an unpatched Apache Struts vulnerability and remained in the environment for 76 days.	A known web-application vulnerability, CVE-2017-5638, was not successfully remediated. Existing scanning and inspection controls failed to identify the exposure and subsequent encrypted malicious activity.

OPM Background Investigation Breach 2014-2015

What happened	How trust was exploited
Background-investigation data affecting about 21.5 million people was stolen, including highly sensitive personnel information.	Attackers obtained credentials and established access inside OPM systems, then moved into databases holding long-lived background-investigation information. The case demonstrates the enduring value of trusted personnel data.

TRUSTED SYSTEMS CASE SERIES

Infrastructure Resilience and Recovery

System trust includes the ability to contain disruption and recover independently. These cases show how internal pathways, engineering access, and recovery architecture shape operational resilience.

NotPetya / Maersk June 2017

What happened	How trust was exploited
Destructive malware spread rapidly across Maersk, disrupting roughly 45,000 PCs and 4,000 servers.	NotPetya entered through the compromised Ukrainian software ecosystem and then moved laterally using stolen credentials, PsExec/WMIC, EternalBlue and EternalRomance across trusted internal networks.

Triton / TRISIS 2017

What happened	How trust was exploited
Malware specifically targeted Schneider Electric Triconex safety instrumented systems at a Saudi petrochemical facility.	Attackers compromised the engineering workstation environment and used the legitimate programming path to interact with SIS controllers, exploiting trust between engineering systems and safety controllers.

Maersk Recovery / Ghana AD 2017

What happened	How trust was exploited
Maersk's recovery from NotPetya depended on a surviving Active Directory domain controller in Ghana.	This was a recovery-trust lesson. Nearly all domain controllers were lost together; the Ghana controller survived because a power outage had taken it offline, providing an accidental independent recovery source.

Volt Typhoon 2021-2024

What happened	How trust was exploited
Chinese state-sponsored actors pre-positioned inside U.S. critical-infrastructure environments for potential future disruption.	The group used valid credentials, compromised infrastructure, and living-off-the-land tools to maintain stealthy access, map networks, and understand pathways toward high-consequence systems.