diamond technologies

Secure Delaware 2021

October 28, 2021

Threats from the Inside

INTRODUCTION

Biography

Duncan Bachen
VP of Security & Architecture

Duncan has been an IT professional for over 25 years, representing local, national, and international organizations. Originally intending to combine his love of film and computers in the special effects industry with a BFA from Ithaca College, Duncan has instead brought his eye for detail and quality to his IT career.

He is a passionate problem solver who likes to think outside the box. Certified as MCSE, MCSA, and MCP, pursuing a CISSP and CEH. In his spare time, he enjoys movies, theater, games, and puzzles of all kinds as well as being active in a medieval recreation group.

diamond technologies

Threats from the Inside

Overview

With the changing security landscape, it's no longer enough to secure the edge of your network. Whether it's malicious actors, your own employees or company culture and policies, the threats are everywhere. "Trust but verify" has now become "Don't trust and assume the worst".

We will provide real world examples of security compromises from inside the company as well as discussing what you should do to mitigate them, including adoption of a zero-trust security model.

- Security breaches from ex-IT
- Impact of company culture on security
- Taking a defensive approach
- What is zero-trust?

diamond technologies

INSIDER THREATS

diamond technologies

Defining the Problem

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

From the US Cybersecurity & Infrastructure Security Agency (CISA):

Insider threat incidents are possible in any sector or organization. An insider threat is typically a current or former employee, third-party contractor, or business partner. In their present or former role, the person has or had access to an organization's network systems, data, or premises, and uses their access (sometimes unwittingly)

diamond technologies

Defining the Problem

Insider threats can pose serious risk to any organization because of the institutional knowledge and trust placed in the hands of the perpetrator. Insider threats can come from current or former employees, contractors, or others with inside knowledge, and the consequences can include compromised sensitive information, damaged organizational reputation, lost revenue, stolen intellectual property, reduced market share, and even physical harm to people.

CISA Executive Assistant Director for Infrastructure Security David Mussington says:

"While security efforts often focus on external threats, often the biggest threat can be found inside the organization"

(https://www.cisa.gov/news/2021/09/28/cisa-releases-new-tool-help-organizations-guard-against-insider-threats 2021/09/28)

diamond technologies

EXAMPLES – DIRECT ATTACKS

Example 1

Source: https://www.justice.gov/usao-edpa/pr/new-jersey-man-sentenced-damaging-employers-computers

FOR IMMEDIATE RELEASE — Wednesday, March 30, 2016

New Jersey Man Sentenced For Damaging Employer's Computers

PHILADELPHIA - Lars Jepsen, 38, formerly of Deptford, NJ, was sentenced yesterday to five months in prison for hacking his former employer's computers. He pleaded guilty on October 29, 2015, to knowingly causing damage to a protected computer and knowingly using the means of identification of another person with intent to commit a crime. In addition to the prison term, U.S. District Court Judge Joseph F. Leeson, Jr., ordered three years of supervised release, with the first six months in home confinement, a $3,000 fine, a $200 special assessment, and restitution of $9,500.

Jepsen damaged the computers of his former employer, after he had been fired. He did this using the username and password of another employee that he had acquired while working on that employee's company computer. Jepsen drove from his New Jersey home to Allentown, PA, where he found an open Internet access point. He used that location to log into the employer's network with the other employee's credentials and then disabled the company's Voice over Internet Protocol (VOIP) telephone network. The company lost its telephone service for several hours.

The case was investigated by the United States Secret Service, and is being prosecuted by Assistant United States Attorney Michael L. Levy.

diamond technologies

Example 1

Timeline

- Password acquired June 23, 2014
  - Employee provided password to work on laptop
- Terminated June 26, 2014
  - All access revoked
- Attack occurred on July 3, 2014
  - Right before holiday

Example 1

Activity

- Used employee password to access VPN
- Used administrative password which was part of automated process (imaging)
- Accessed VOIP console and deleted all phone numbers and routing

Example 1

Countermeasures

- Drove to remote location
- Used another employee credentials
- Uninstalled VPN software

Example 1

Evidence

- VPN logs
  - Previous IP addresses of both employees
- System logs
  - Able to track movement through various devices
- Communication logs
  - Warrant to get WiFi access records
- PC Registry
  - Remnants of removal

diamond technologies

Example 1

Process and lessons learned

- Reported to FBI, referred to Secret Service
- 2-year investigation
- Quickly gathering logs before they disappeared
- Employee sharing with “trusted” individual
- Edge protection not enough
- Material Loss vs True Loss
- How many administrative passwords do you have?

diamond technologies

Example 2

Source: https://www.justice.gov/usao-de/pr/middletown-man-sentenced-six-months-home-confinement-damaging-former-employers-computer

FOR IMMEDIATE RELEASE — Wednesday, June 9, 2021

Middletown Man Sentenced To Six Months of Home Confinement For Damaging Former Employer's Computer Network

WILMINGTON, Del. – David C. Weiss, United States Attorney for the District of Delaware, announced today that Levii Delgado, 36, of Middletown, was sentenced today to six months of home confinement and over $13,000 in restitution by the Honorable Leonard P. Stark, Chief United States District Judge for the District of Delaware. Delgado pled guilty in February 2021 to one count of causing damage to a protected computer.

According to court documents, Delgado worked as an Information Technology (IT) administrator at a medical center that provides care to under-served communities. The medical center terminated Delgado's employment in August 2017. Following that termination, Delgado was no longer authorized to access the medical center's computer network and his credentials that had allowed him to access the medical center's network were disabled. Four days after his termination, Delgado connected a personal laptop to the medical center's computer network through an administrator account that Delgado continued to use without authorization. Once Delgado gained unauthorized access to the computer network, he caused the deletion of the medical center's employee user accounts, the disabling of its computer accounts, and the deletion of its file server. Delgado's actions prevented the medical center's employees from logging into their computers and accessing patient files necessary to conduct operations. As a result, the medical center's ability to see and treat its patients was impaired.

No patient information was compromised or accessed as a result of Delgado's actions.

U.S. Attorney Weiss stated, "The defendant abused his knowledge of his former employer's computer network to deliberately disrupt the medical center's capability to conduct business. As a result, the defendant directly impeded that entity's ability to provide medical care to the communities it serves, putting patients at risk. My office is committed to prosecuting any individual who thinks attacking a former employer's computer network is an acceptable reaction to getting fired."

"What Mr. Delgado did was not only intentional, reckless and petty, but also caused a severe disruption in medical care in an underserved community," said Rachel Byrd, Acting Special Agent in Charge of the FBI Baltimore Field Office. "Computer intrusion is a crime and the FBI, and our law enforcement partners, will continue to pursue those who compromise, mishandle or disrupt computer networks."

This case was investigated by the FBI-Baltimore Division's Cyber Task Force and was prosecuted by Assistant U.S. Attorney Jesse S. Wenger.

Cyberattacks are on the rise. A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. Federal Government agencies work together to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities to minimize asset vulnerability and bring malicious actors to justice. Private sector entities are encouraged to report a cyber incident to the FBI at 1-800-CALLFBI (225-5324) or file a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov.

A copy of this press release is located on the website of the U.S. Attorney's Office for the District of Delaware. Related court documents and information is located on the website of the District Court for the District of Delaware or on PACER.

diamond technologies

Example 2

Timeline

- Terminated August 2017
  - All access revoked
- Attack occurred 4 days later

Example 2

Activity

- Used secondary administrator password not changed
- Accessed Wi-Fi from parking lot with personal laptop
- Deleted all user accounts, disabled all computer accounts, and deleted file server

diamond technologies

Example 2

Countermeasures

- Used another administrative account
- Used common access of local Wi-Fi
- Salt the earth, destroy everything

Example 2

Evidence

- VPN logs
  - Showed previous use of compromised account
- NPS logs
  - Network Policy server used for AD based access to Wi-Fi
- Domain and system event logs
  - Activity of lateral movement and actions taken on domain objects

diamond technologies

Example 2

Process and lessons learned

- Reported to FBI
- 3.5-year investigation
- Quickly gathering logs before they disappeared
- Secondary methods of system access, not just remote
- Impact not only to business but to patients
- Rarely used backup admin accounts

COMPANY CULTURE

Company Culture

Your company culture has a direct impact on the internal risks

- Unhappy employees are less likely to pay attention to details.
- A sustainable security culture is persistent. It's not a once-a-year event, it's part of everything you do.
- In any system, humans are always the weakest link
- People generally want to do the right thing; they just need to be taught
- Goal is to reduce risk, but you still need processes and policies in place for auditing and compliance.

Is your company culture toxic? Think about how many of these things are true in your organization

diamond technologies

Company Culture

- Playing the blame game. Looking for a scapegoat.
  - It's ok to make mistakes. Better than hiding them. Hard to do when in constant fear of losing your job
- Fear of appearing incorrect when asking questions
  - Actions without verification
- Cynicism towards management
  - Not trusting the tools, processes, policies and procedures
- Is "no" the first answer? Workarounds and shortcuts
  - Do it the easy way. Don't bother with security

diamond technologies

Company Culture

- Is IT/Security in a silo?
  - Not part of the team
- Ongoing security training?
  - Is it mandatory? How effective is it?
- Overworked or burned out
  - High employee turnover
- Proper budget for updated/new systems
  - Productivity, security risks, company reputation

diamond technologies

Company Culture

- Poor communication skills
  - Doing “something” but not doing it right, or doing nothing at all
- Lack of diversity
  - Only seeing one side of a problem
- Too much trust in technology
  - Assumption that everything is safe

EXAMPLES – INDIRECT ATTACKS

Examples

Fear of being wrong or asking owner to confirm

Employee purchased gift cards

- Multiple different companies. Not an isolated incident. Hundreds of dollars worth.

From: Adam [mailto:ceo@execipad.com]
Sent: Wednesday, January 23, 2019 8:20 AM
To: Dave
Subject: RE: Hi Dave

Hi
The type of card I need is Google play cards . $500 denomination, I need $500 X 4cards You can purchase on-line www.giftcards.com or from the store.Scratch out the back to reveal the card codes, and email me the codes from the store of purchase

Thanks
sent from my ipad

On January 23, 2019 at 6:47 PM Dave <dave@> wrote:

I am at office now. let me know what you need, I can get gift cards at CVS up the street

Dave

Examples

- Spoofed email
  - One and done
- Compromised email
  - Direct interaction with the employee who replies
- Pick up the phone and talk to someone
- Letting your guard down and not noticing the indicators
  - Wrong email
  - Strange requirements

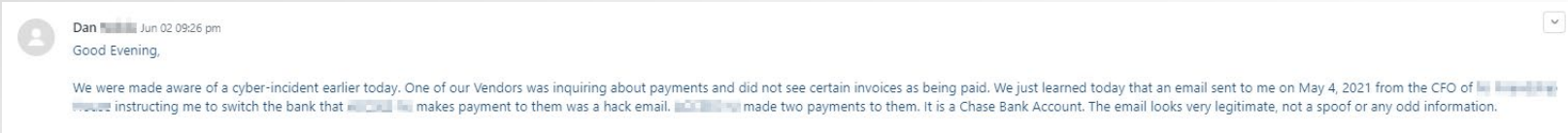
Examples

- Fear of appearing incorrect when asking questions

- Too much trust in technology

Customer authorized funds transfer to new bank account for payment

- Multiple different companies. Not an isolated incident. Thousands of dollars worth



Dan [redacted] Jun 02 09:26 pm

Good Evening,

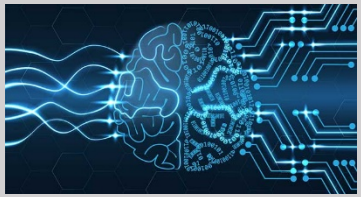
We were made aware of a cyber-incident earlier today. One of our Vendors was inquiring about payments and did not see certain invoices as being paid. We just learned today that an email sent to me on May 4, 2021 from the CFO of [redacted] instructing me to switch the bank that [redacted] makes payment to them was a hack email. [redacted] made two payments to them. It is a Chase Bank Account. The email looks very legitimate, not a spoof or any odd information.

Examples

- Changes to payment should be flagged and communicated via phone
- Can go unnoticed for some time
- Downstream effects
  - Stop everything and prioritize
  - Additional costs for investigation of larger compromise
  - Additional costs for legal involvement
  - Additional costs for preservation of documents
  - Additional insurance costs in the future

diamond technologies

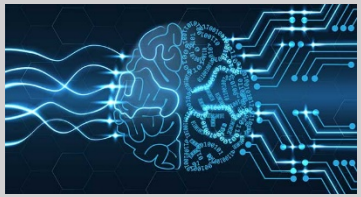
WHAT TO DO



Continual Improvement

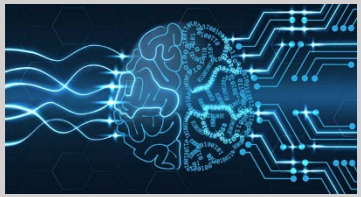
- Conduct a postmortem after an event. What worked well? What didn't work well? What needs to change?
- How is the security landscape changing? Can my existing products cover the new threat models?
- Layered approach. Keep building the defenses
- Test and train your systems. Test and train your staff.
- Eliminate toxic culture one step at a time
- Include questions about IT and culture in exit interviews

diamond technologies



Defensive Approach

- Ensure that logging is in place for all modifications and activity throughout your organization
- Utilize logging solutions such as syslog to provide long term storage of logs in a centralized location
- Take advantage of a SIEM (security information and event manager) to supplement your staff and automate the correlation and analyzing of events to help identify threats. If possible, establish automatic rules which can perform actions on your behalf when something anomalous is detected.
- Track use of shared administrative credentials and identify potential ingress and egress points



Defensive Approach

- The standard defenses already discussed are simply not enough.
- They are designed to be permissive, and as a result, tend to have gaps or are overly broad.

diamond technologies

ZERO-TRUST

diamond technologies

Zero-Trust

Crowdstrike defines Zero Trust as:

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

This framework is defined by various industry guidelines such as Forrester eXtended, Gartner's CARTA, and more recently NIST 800-207, as an optimal way to address current security challenges for a cloud-first, work from anywhere world.

diamond technologies

Zero-Trust

As per NIST Special Publication 800-207:

"This complexity has outstripped legacy methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise. Perimeter-based network security has also been shown to be insufficient since once attackers breach the perimeter, further lateral movement is unhindered."

"Zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different—or no more trustworthy—than any nonenterprise-owned environment. In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks."

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

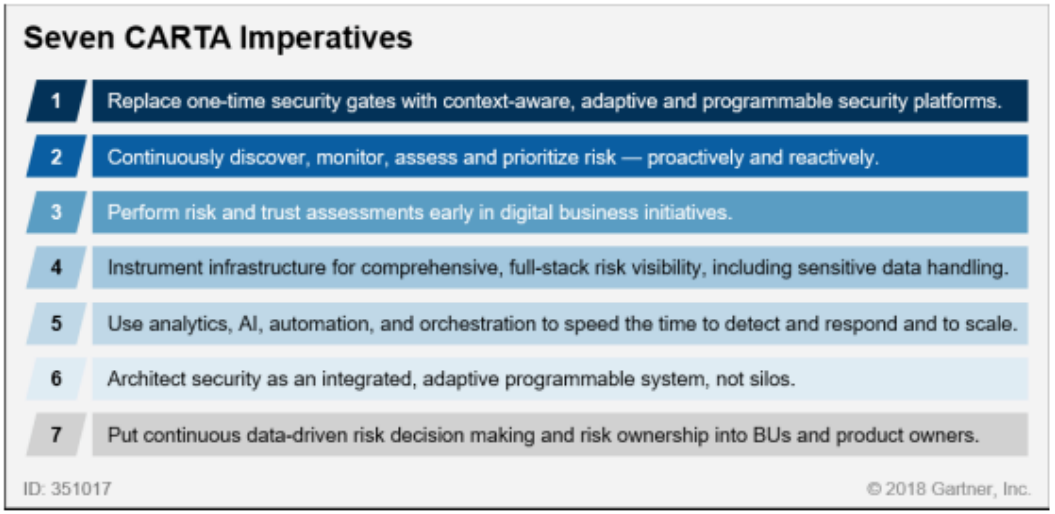
diamond technologies

Zero-Trust

Source: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Forcepoint/Forcepoint-1-4YCDU8P.pdf

Security and risk management leaders need to embrace a strategic approach where security is adaptive, everywhere, all the time. Gartner called this strategic approach "continuous adaptive risk and trust assessment," or CARTA.

Seven CARTA Imperatives



Source: Gartner (April 2018)

diamond technologies

Zero-Trust

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

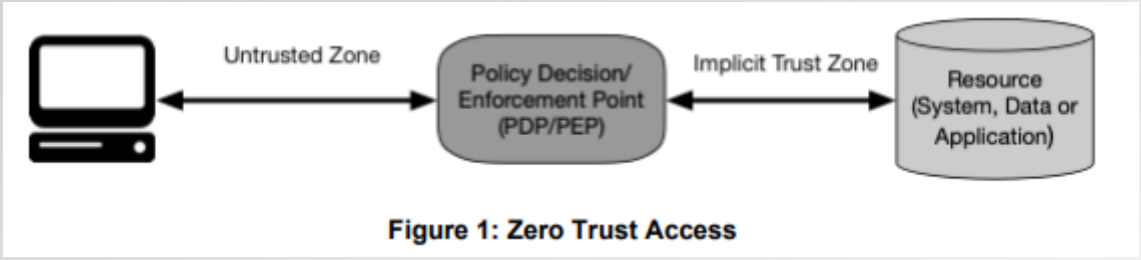


Figure 1: Zero Trust Access

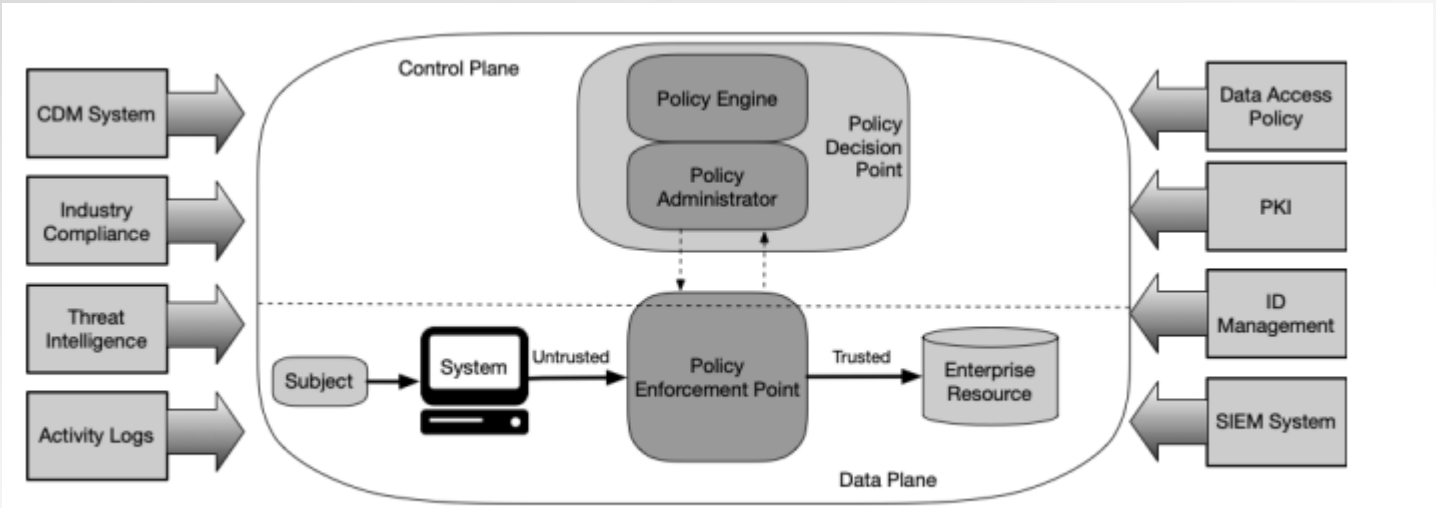


Figure 2: Core Zero Trust Logical Components

Zero-Trust

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Basic Tenants

1) All data sources and computing services are considered resources.

2) All communication is secured regardless of network location.

3) Access to individual enterprise resources is granted on a per-session basis.

4) Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

5) The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

7) The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

diamond technologies

Zero-Trust

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Assumption for network connectivity

1) The entire enterprise private network is not considered an implicit trust zone
2) Devices on the network may not be owned or configurable by the enterprise.
3) No resource is inherently trusted
4) Not all enterprise resources are on enterprise-owned infrastructure.
5) Remote enterprise subjects and assets cannot fully trust their local network connection.
6) Assets and workflows moving between enterprise and nonenterprise infrastructure should have a consistent security policy and posture.

diamond technologies

CISA INSIDER RISK MITAGATION

diamond technologies

Tools

Source: https://www.cisa.gov/news/2021/09/28/cisa-releases-new-tool-help-organizations-guard-against-insider-threats

The Cybersecurity and Infrastructure Security Agency (CISA) released an Insider Risk Mitigation Self-Assessment Tool (for best results, please download and open with Adobe) today, which assists public and private sector organizations in assessing their vulnerability to an insider threat. By answering a series of questions, users receive feedback they can use to gauge their risk posture. The tool will also help users further understand the nature of insider threats and take steps to create their own prevention and mitigation programs.

https://www.cisa.gov/sites/default/files/publications/IRMPE_Assessment_v1_2021-08-25.pdf

Resources

https://www.cisa.gov/insider-threat-mitigation

The key steps to mitigate insider threat are Define, Detect and Identify, Assess, and Manage.

https://www.cisa.gov/publication/insider-threat-mitigation-resources

Insider Threat Mitigation Guide	5.4 MB
HRs Role in Preventing Insider Threats Fact Sheet	404.01 KB
Insider Threat 101 Fact Sheet	491.85 KB
Fact Sheet - Insider Threat Mitigation Program	490.01 KB
Pathway to Violence: Warning Signs and What You Can Do	623.3 KB
Insider Threat	447.96 KB
Combating the Insider Threat	97.24 KB
NITTF Insider Threat Guide	4.01 MB
NITTF Maturity Framework	5.54 MB

Threats from the Inside

Thanks for coming!