Tackling Mainframe Insider Threats: The 5 Top Threats to Consider

Ray Overby

Distinguished Engineer, Security

Rocket® software

What is An Insider Threat

- An insider threat is a security risk that comes from within your organization.
- Employees, partners, vendors, interns, suppliers or contractors can potentially become an insider threat.
- These people can access your organization's internal network and may accidentally leak or purposely steal sensitive information.

Top 5 Insider Threat Personas

Departing employees: Employees leaving the company voluntarily or involuntarily are among the most common insider threats. They might take materials they're proud of to help land a new job or, more viciously, steal and expose sensitive data out of revenge.

Malicious insiders: These individuals are current employees. They might not be your company's biggest fans and usually act on their grievances by altering or deleting crucial data sets, disclosing secret information or engaging in other types of sabotage.

Security evaders: Modern companies have security policies for safeguarding their essential data. Some workers can find these protections inconvenient, leading them to create workarounds that increase the chances of a data breach.

Top 5 Insider Threat Personas

Inside agents: These threats work on behalf of an external group, whether knowingly or unknowingly. Outsiders may compel them to give information through blackmail or bribery or deceive them into sharing their login credentials through **social engineering**.

Third Party Partners: Not all insiders are on the payroll. Suppliers, contractors, vendors and other external parties with some level of inside access can be just as dangerous as employees with the same permissions.

Critical Insider Threats to Manage

Here are the most critical insider threats to manage:

- ✓ **Malicious Insiders (Data Theft & Sabotage)**: Employees, contractors, or partners who deliberately misuse their authorized access to steal intellectual property, customer data, or sabotage systems for financial gain or revenge.

- ✓ **Negligent/Careless Insiders (Data Exposure)**: Employees who fail to follow security protocols, such as using weak passwords, misconfiguring cloud systems, or mishandling sensitive data, which can lead to accidental exposure.

Here are the most critical insider threats to manage:

- ✓ **Compromised Users (Credential Theft):** Legitimate user credentials stolen by external attackers through phishing or malware, allowing hackers to operate within the network undetected.

- ✓ **Unauthorized Usage of GenAI Tools:** 76% of organizations report employees using generative AI tools without authorization, leading to potential leaks of sensitive company information

Here are the most critical insider threats to manage:

- ✓ **Privilege Misuse:** Users with elevated access (administrators, IT staff) accessing data or systems beyond their scope of duty.

- ✓ **Exfiltration of IP via Removable Media/Cloud:** The unauthorized transfer of sensitive information to personal USB drives, email accounts, or cloud storage platforms

Real World Examples

Real-Life Examples of Insider Threats

The former Tesla employees who leaked PII data to a foreign media outlet.

- Tesla suffered a major data breach that was orchestrated by two former employees, who leaked sensitive personal data to a foreign media outlet.
- The leaked information included names, addresses, phone numbers, employment records, and social security numbers of over 75,000 current and former employees.
- The insider breach also exposed customer bank details, production secrets, and complaints about Tesla’s Full Self-Driving features.

Real-Life Examples of Insider Threats

The departing employee at Yahoo who stole trade secrets.

- In May of 2022, a research scientist at Yahoo named Qian Sang stole proprietary information about Yahoo's AdLearn product minutes after receiving a job offer from The Trade Desk, a competitor.
- He downloaded approximately 570,000 pages of Yahoo's intellectual property (IP).
- Yahoo realized that Sang had stolen data (and a competitive analysis of The Trade Desk) a few weeks after the incident and sent him a cease-and-desist letter.
- Yahoo has brought three separate charges against Sang, including theft of IP data. Yahoo claims that Sang's actions divested it of the exclusive control of its trade secrets, information that would give competitors an immense advantage.

Real-Life Examples of Insider Threats

The departing Proofpoint employee who enriched a competitor

- In July 2021, Samuel Boone, an employee of Proofpoint, stole confidential sales enablement data before starting a new job at Abnormal Security.
- Proofpoint's own solution for preventing data loss (DLP) didn't hinder the employee from downloading high-value documents to a USB drive and sharing them.
- Months later, Proofpoint discovered that he had taken the files. At that point, Boone made substantial headway in channel sales at Abnormal Security.
- Proofpoint sued him in federal court for unlawfully sharing battlecards that would give him and his employer an unfair advantage.

Real-Life Examples of Insider Threats

The third-party vendor to Marriott whose app had a vulnerability

- The adverse effects of data breaches don’t just apply to your company — they can also extend to your customers.
- In January 2020, cyber attackers exploited the credentials of two Marriott employees to hack an application the company used as part of their guest services. The attackers stole over 5 million guest records, including people’s contact information, gender, birthdays and loyalty account numbers.
- By the way, this was a mainframe breach.
- While Marriott quickly reacted once it discovered the breach, it didn’t notice the suspicious activity for nearly two months. The company had to pay a £18.4 million fine for exposing the sensitive data of approximately 339 million guests and failing to comply with GDPR.

Real-Life Examples of Insider Threats

The security evader at Boeing who sent company data to a personal email account

- Sometimes seemingly harmless actions pose a significant security risk.
- In 2017, an employee at global aerospace company Boeing emailed a spreadsheet to his wife — who wasn't an employee — hoping she could help him resolve formatting issues.
- Unbeknownst to the employee, the spreadsheet contained the personal information of approximately 36,000 of his coworkers in hidden columns. By bypassing security protocols and sending the spreadsheet to an unsecured device and non-employee, he compromised employee ID, place of birth and social security number information.
- While Boeing is confident the data didn't move beyond those two devices, it offered all affected employees two years of free credit monitoring – which is an estimated $7 million in payments.

Real-Life Examples of Insider Threats

The security evader at Boeing who sent company data to a personal email account

- Sometimes seemingly harmless actions pose a significant security risk.
- In 2017, an employee at global aerospace company Boeing emailed a spreadsheet to his wife — who wasn't an employee — hoping she could help him resolve formatting issues.
- Unbeknownst to the employee, the spreadsheet contained the personal information of approximately 36,000 of his coworkers in hidden columns. By bypassing security protocols and sending the spreadsheet to an unsecured device and non-employee, he compromised employee ID, place of birth and social security number information.
- While Boeing is confident the data didn't move beyond those two devices, it offered all affected employees two years of free credit monitoring – which is an estimated $7 million in payments.

High-Impact Training Methodologies

To ensure retention and behavioral change, 2026 best practices emphasize:

- ✓ **Role-Based Training (RBT): Customizing content to an employee's specific job function. For example, finance teams receive training on wire transfer fraud, while developers focus on secure coding and API vulnerabilities.**
- ✓ **Micro-Learning & Gamification: Using short, frequent modules (5 minutes or less) rather than long, annual sessions to keep security top-of-mind.**
- ✓ **Contextual Feedback: Providing immediate, "interventional" feedback when a user makes a mistake, such as clicking a simulated phishing link, to reinforce the lesson in real-time.**

Thank you

roverby@rocketsoftware.com

Rocket® software