2018 Anchorage Regional Compliance Conference

Access, Security, And Audits – Oh My!

- Defining Insider Threat
- Surprising Statistics
- Insider Threat Behaviors
- Working with your IT Department

Briefer: Ute Kragl, DoD Compliance Officer

---

2018 Anchorage Regional Compliance Conference

Defining the Threat

Who is an Insider?
- A current or former employee, contractor, or business partner who has or had authorized access to the organization’s network, systems, and/or data.

Employees:
- Privileged users, such as IT team members and Super Users
- Knowledge workers, such as analysts or developers
- Resigned or terminated employees
- Employees involved in a merger or acquisition

Third Parties:
- Vendors
- Contractors
- Partners
Defining the Threat

What is an Insider Threat?
- An insider threat happens when someone who is close to an organization, and who has authorized access, misuses that access to negatively impact the organization’s critical information or systems.

<table>
<thead>
<tr>
<th>Inadvertent:</th>
<th>Malicious:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Human error</td>
<td>♦ Sabotage</td>
</tr>
<tr>
<td>♦ Bad judgment</td>
<td>♦ Intellectual property theft</td>
</tr>
<tr>
<td>♦ Unintentional aiding and</td>
<td>♦ Espionage</td>
</tr>
<tr>
<td>abetting</td>
<td>♦ Fraud (financial gain)</td>
</tr>
<tr>
<td>♦ Phishing</td>
<td></td>
</tr>
<tr>
<td>♦ Malware</td>
<td></td>
</tr>
<tr>
<td>♦ Stolen credentials</td>
<td></td>
</tr>
<tr>
<td>♦ Convenience</td>
<td></td>
</tr>
</tbody>
</table>

70% is the annual reported average of insider threats by enterprise security executives.
What do employees have access to?

62% of business personnel report they have access to data they probably should not see/have.

**Speed of Detection**

43% is how quickly an organization is able to detect employees accessing files and emails they were not authorized to see.
32% - Nearly one third of all organizations still have **no capability** to prevent or deter insider incident or attack.

9% of respondents rank their prevention methods as **very effective**
45% of IT executives say malicious insider attacks is one of the email security risks they are most ill-prepared to cope with.

45% of employees looking to establish a second stream of income off of their employer's sensitive data.
Stopping Insider Threat!

Mission Impossible…

...People will be people, unintentional or with malicious intent.

However, there are behaviors that “could” indicate Insider Threat

2018 Anchorage Regional Compliance Conference

CitiBank take down…

One Texas man who worked at Citibank was able to take down connectivity to approximately 90% of all Citibank networks in North America by erasing the configuration files for nine routers in Citibank’s global network operations center.

The Trigger?

- Incident was due to a “poor performance review”
Insider Threat Motivators: 3 Most Common Insider Threats

1 – Modifying or stealing confidential or sensitive information for personal gain.
2 – Theft of trade secrets or customer information to be used for business advantage or to give to a foreign government or organization.
3 – Sabotage of an organization’s data, systems, or networks. (retaliation / or the above)

Behavior that “could” indicate Insider Threat

<table>
<thead>
<tr>
<th>Characteristics of Insiders at Risk of Becoming a Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introversion</td>
</tr>
<tr>
<td>Greed / Financial need</td>
</tr>
<tr>
<td>Vulnerable to blackmail</td>
</tr>
<tr>
<td>Compulsive and destructive</td>
</tr>
<tr>
<td>Rebellious, passive aggressive</td>
</tr>
<tr>
<td>Ethical “flexibility”</td>
</tr>
<tr>
<td>Reduced loyalty</td>
</tr>
<tr>
<td>Entitlement – narcissism</td>
</tr>
<tr>
<td>(ego / self-image)</td>
</tr>
</tbody>
</table>
Indicators of Malicious Threat Activity

- Remotely accesses the network while on vacation, sick or at odd times
- Works odd hours without authorization
- Notable enthusiasm for overtime, weekend or unusual work schedules
- Unnecessarily copies material, especially if it is proprietary or classified
- Interest in matters outside of the scope of their duties
- Signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behavior, should trigger concern.

Be on the look out for warning signs among employees such as acquisition of unexpected wealth, unusual foreign travel, irregular work hours or unexpected absences.

Reviewing your Compliance Program

Some things to consider as you build, improve, or revalidate your compliance program:

- **Detect Insider Threats** – Uncover risky user activity by identifying anomalous behavior.
- **Investigate Incidents** – Investigate suspicious user activity in minutes, not days.
- **Prevent Incidents** – Reduce risk with real-time user notifications and blocking.
- **Protect User Privacy** – Anonymize user data to protect employee and contractor privacy and meet regulations.
- **Satisfy Compliance** – Meet key compliance requirements regarding insider threats in a streamlined manner.
- **Integrate Tools** – Integrate insider threat detection combined with the right threat detection tools for your network and work environment.
Identifying the Threat – Risk Assessment

Statistics you need to be aware of:

- **36%** - careless/ignorant users who cause inadvertent security breaches
- **52%** - employees see no security risk when sharing work logins
- **19%** - employees stated they were involved (offender) in a security breach
- **86%** - IT professionals consider insider threat a cultural issue
- **29%** - employees did not have a security policy in place
- **2500** – daily internal security breaches

Knowing the Risk - Where Compliance & IT Merge

**Insider Threat is defined as:**

- An insider threat happens when someone who is close to an organization, and who has authorized access, misuses that access to negatively impact the organization’s critical information or systems.

- **Employees (incl. Managers)**
  - Type of access
  - Level of access
  - Computer skills

- **Network Security**
  - Credentials to access
  - Password access
  - Partition access

- **IT Support Personnel**
  - Type of access
  - Level of access
  - Authorization to access

- **Distribution & Dissemination**
  - Emails (distro lists, aliases)
  - Compartmented data
  - Need to know
### Top 25 Most Common Passwords

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>password</td>
<td>password</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
</tr>
<tr>
<td>2</td>
<td>123456</td>
<td>123456</td>
<td>password</td>
<td>password</td>
<td>password</td>
<td>password</td>
<td>password</td>
</tr>
<tr>
<td>3</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
</tr>
<tr>
<td>4</td>
<td>master</td>
<td>abc123</td>
<td>master</td>
<td>master</td>
<td>master</td>
<td>master</td>
<td>master</td>
</tr>
<tr>
<td>5</td>
<td>abc123</td>
<td>monkey</td>
<td>abc123</td>
<td>monkey</td>
<td>abc123</td>
<td>monkey</td>
<td>abc123</td>
</tr>
<tr>
<td>6</td>
<td>monkey</td>
<td>monkey</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
</tr>
<tr>
<td>7</td>
<td>123456</td>
<td>letmein</td>
<td>111111</td>
<td>1234</td>
<td>football</td>
<td>123456</td>
<td>123456</td>
</tr>
<tr>
<td>8</td>
<td>letmein</td>
<td>dragon</td>
<td>123456</td>
<td>baseball</td>
<td>1234</td>
<td>123456</td>
<td>123456</td>
</tr>
<tr>
<td>9</td>
<td>trustno1</td>
<td>111111</td>
<td>iloveyou</td>
<td>dragon</td>
<td>123456</td>
<td>princess</td>
<td>football</td>
</tr>
<tr>
<td>10</td>
<td>dragon</td>
<td>baseball</td>
<td>adobe123</td>
<td>football</td>
<td>baseball</td>
<td>1234</td>
<td>iloveyou</td>
</tr>
<tr>
<td>11</td>
<td>baseball</td>
<td>iloveyou</td>
<td>123123</td>
<td>123456</td>
<td>welcome</td>
<td>admin</td>
<td>welcome</td>
</tr>
<tr>
<td>12</td>
<td>111111</td>
<td>trustno1</td>
<td>admin</td>
<td>monkey</td>
<td>123456</td>
<td>welcome</td>
<td>welcome</td>
</tr>
<tr>
<td>13</td>
<td>iloveyou</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>letmein</td>
<td>abc123</td>
<td>solo</td>
</tr>
</tbody>
</table>

*Top 25 most common passwords by year according to SplashData*
Strong Passwords

A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase.

Yx4!7rTo0$je1*bq

This is assigned to you – will you remember it tomorrow?

Strong Passwords

The key aspects of a strong password are length (the longer the better); a mix of letters (upper and lower case), numbers, and symbols; with no ties to your personal information, and no dictionary words. ... The secret is to make passwords memorable but hard to guess.

e@rThqU@k3
W0lf&B@e@r=Fi$hing
Q12we#$R56ty&*U90io
There is much more you & your IT department can do!

- **Identify** where protected data is stored
- **Review** systems, applications, and platforms that store data
- **Determine** how to best meet compliance standard
- **Training** on how to protect sensitive data
  - Include security policies and procedures
  - Include all personnel in training
- **Invest** in (automated) tools that monitor system access & usage
- **Implement** auditing policy, process, & practice
  - Requires visibility into who has access, who is using access, and what actions are being taken to protect the data

---

**Access, Security, And Audits – Oh My!**

- Defining Insider Threat
- Surprising Statistics
- Insider Threat Behaviors
- Working with your IT Department

**Questions?**