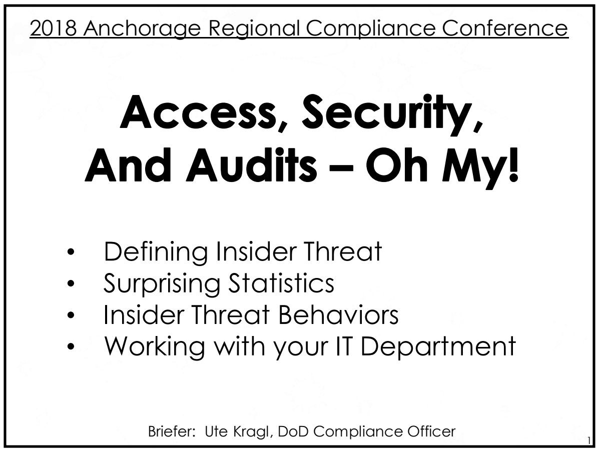
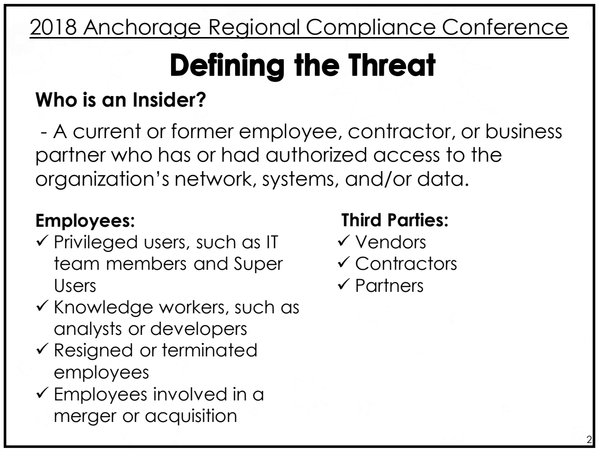


Access, Security, And Audits – Oh My!

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

Briefer: Ute Kragl, DoD Compliance Officer



Defining the Threat

Who is an Insider?

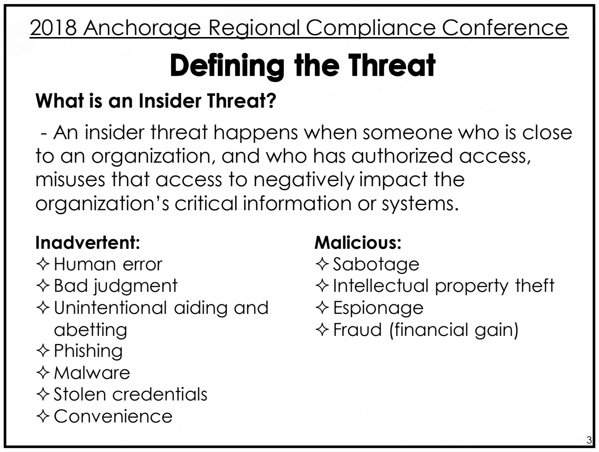
- A current or former employee, contractor, or business partner who has or had authorized access to the organization's network, systems, and/or data.

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.

Inadvertent:

✧ Human error
✧ Bad judgment
✧ Unintentional aiding and abetting
✧ Phishing
✧ Malware
✧ Stolen credentials
✧ Convenience

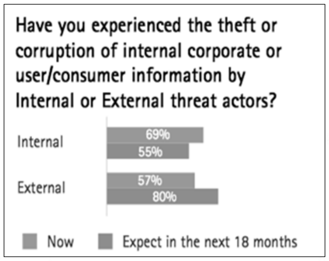
Malicious:

✧ Sabotage
✧ Intellectual property theft
✧ Espionage
✧ Fraud (financial gain)

2018 Anchorage Regional Compliance Conference

Surprising or Disturbing Statistics About Insider Threat

70% is the annual reported average of insider threats by enterprise security executives.

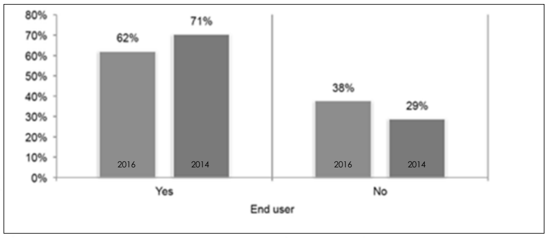

Have you experienced the theft or corruption of internal corporate or user/consumer information by Internal or External threat actors?

4

2018 Anchorage Regional Compliance Conference

What do employees have access to?

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

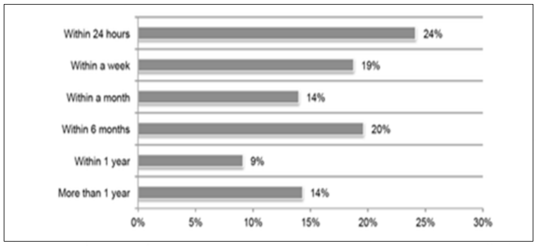


5

2018 Anchorage Regional Compliance Conference

Speed of Detection

43% is how quickly an organization is **able to detect** employees accessing files and emails they were not authorized to see?



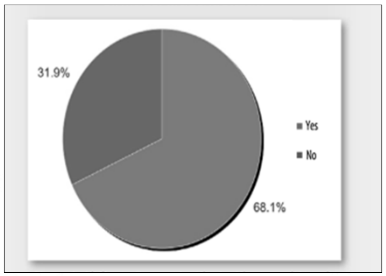
IT statistics only

6

2018 Anchorage Regional Compliance Conference

Prevention Capability?

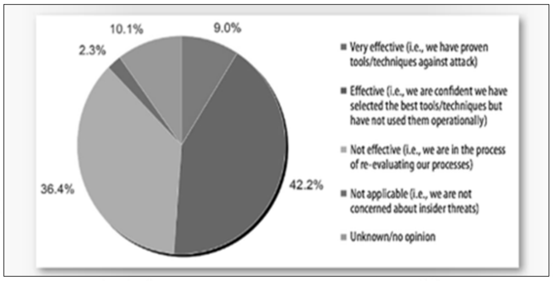
32% - Nearly one third of all organizations still have **no capability** to prevent or deter insider incident or attack.



2018 Anchorage Regional Compliance Conference

Effectiveness of Measures?

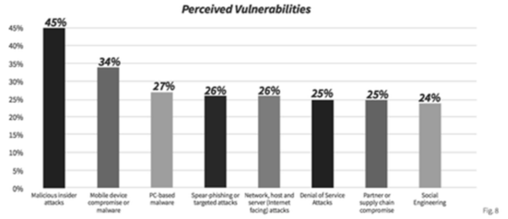
9% of respondents rank their prevention methods as **very effective**



2018 Anchorage Regional Compliance Conference

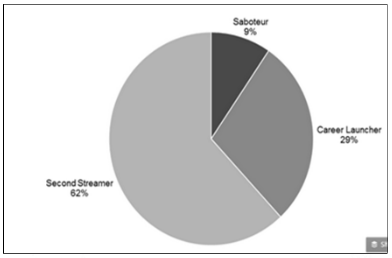
Perceived Vulnerabilities

45% of IT executives say **malicious insider attacks** is one of the email security risks they are most ill-prepared to cope with.



Type of Insider Threat

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.

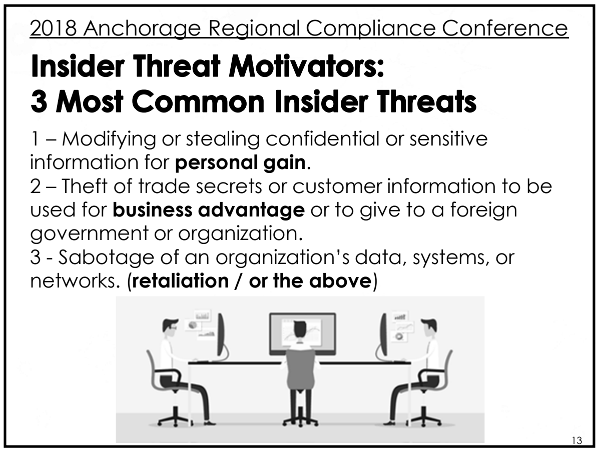
However, there are behaviors that "could" indicate Insider Threat

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.

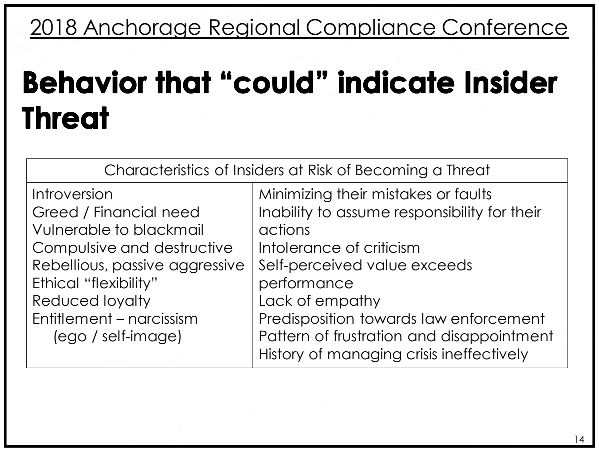
The Trigger?

- Incident was due to a "poor performance review"



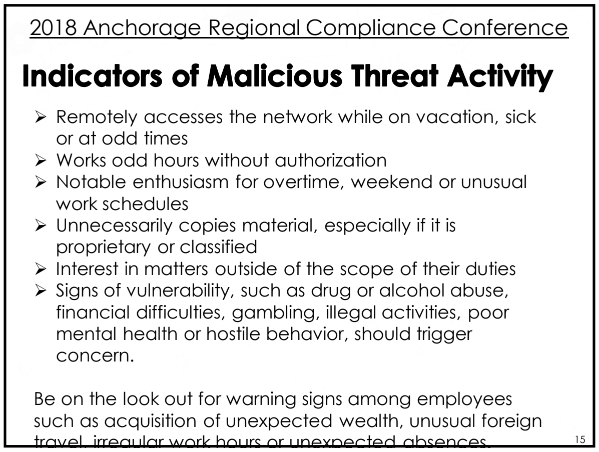
Insider Threat Motivators: 3 Most Common Insider Threats

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

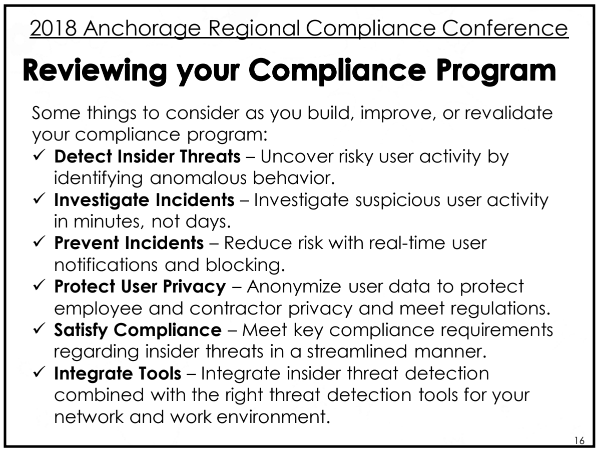
Characteristics of Insiders at Risk of Becoming a Threat	
Introversion Greed / Financial need Vulnerable to blackmail Compulsive and destructive Rebellious, passive aggressive Ethical "flexibility" Reduced loyalty Entitlement – narcissism (ego / self-image)	Minimizing their mistakes or faults Inability to assume responsibility for their actions Intolerance of criticism Self-perceived value exceeds performance Lack of empathy Predisposition towards law enforcement Pattern of frustration and disappointment History of managing crisis ineffectively



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.



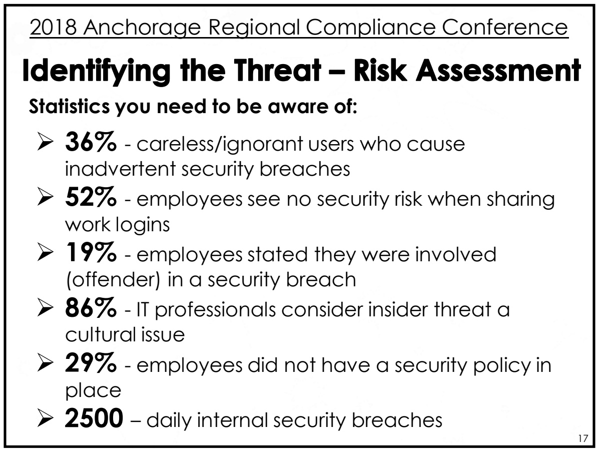
2018 Anchorage Regional Compliance Conference

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.

16



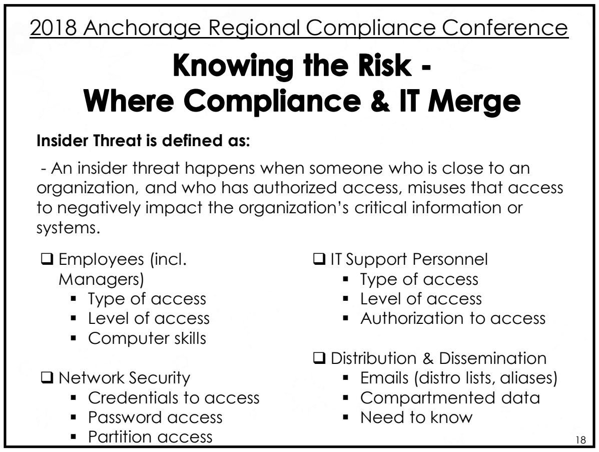
2018 Anchorage Regional Compliance Conference

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

17



2018 Anchorage Regional Compliance Conference

Knowing the Risk -
Where Compliance & IT Merge

Insider Threat is defined as:

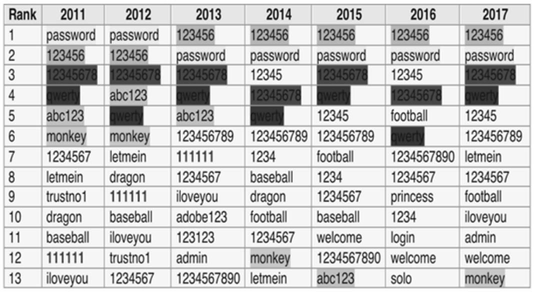
- An insider threat happens when someone who is close to an organization, and who has authorized access, misuses that access to negatively impact the organization's critical information or systems.

- ❑ 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

18

2018 Anchorage Regional Compliance Conference

25 Most Common Passwords

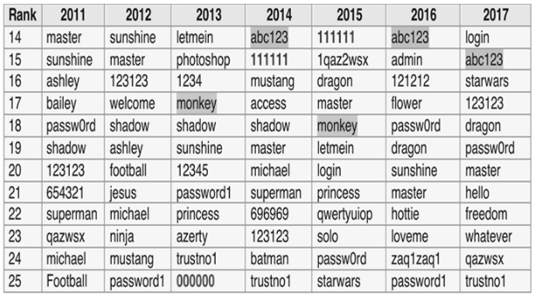


Rank	2011	2012	2013	2014	2015	2016	2017
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey

Top 25 most common passwords by year according to SplashData

2018 Anchorage Regional Compliance Conference

25 Most Common Passwords



Rank	2011	2012	2013	2014	2015	2016	2017
14	master	sunshine	letmein	abc123	111111	abc123	login
15	sunshine	master	photoshop	111111	1qaz2wsx	admin	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars
17	bailey	welcome	monkey	access	master	flower	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd
20	123123	football	12345	michael	login	sunshine	master
21	654321	jesus	password1	superman	princess	master	hello
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx
25	Football	password1	000000	trustno1	starwars	password1	trustno1

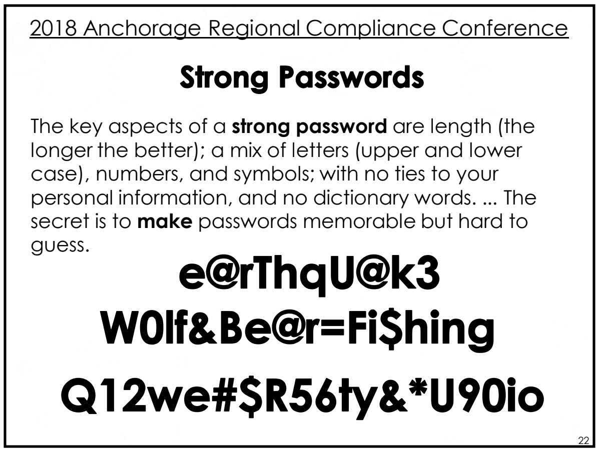
2018 Anchorage Regional Compliance Conference

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?



2018 Anchorage Regional Compliance Conference

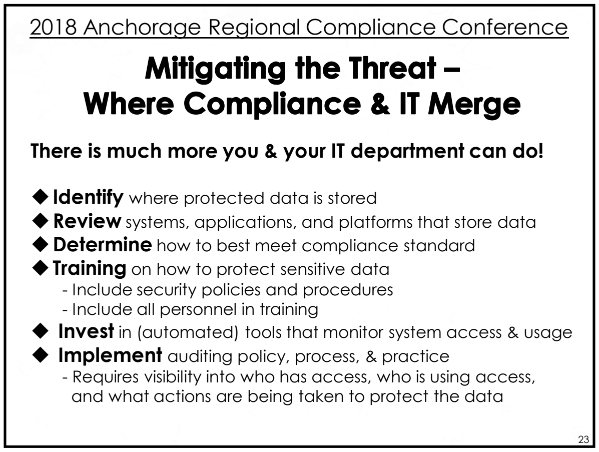
Strong Passwords

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&Be@r=Fi$hing

Q12we#$R56ty&*U90io

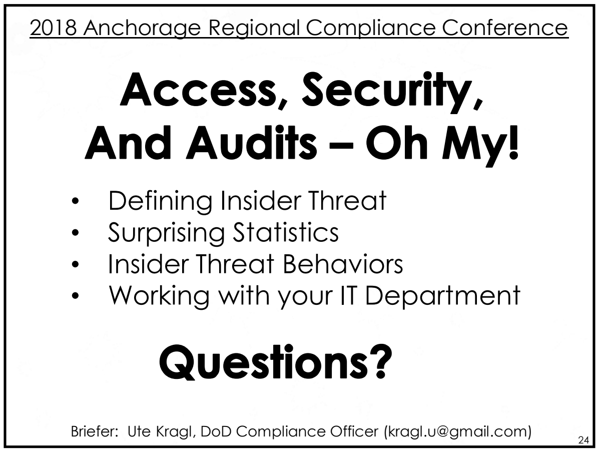


2018 Anchorage Regional Compliance Conference

Mitigating the Threat – Where Compliance & IT Merge

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



2018 Anchorage Regional Compliance Conference

Access, Security, And Audits – Oh My!

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

Questions?

Briefer: Ute Kragl, DoD Compliance Officer (kragl.u@gmail.com)