Alaska Power Association
Alaska Electric Utility
Accounting and Finance Workshop

Cybersecurity Fundamentals

ARCTIC IT
Tenacious Ingenuity™

Tuesday, October 9th, 2018

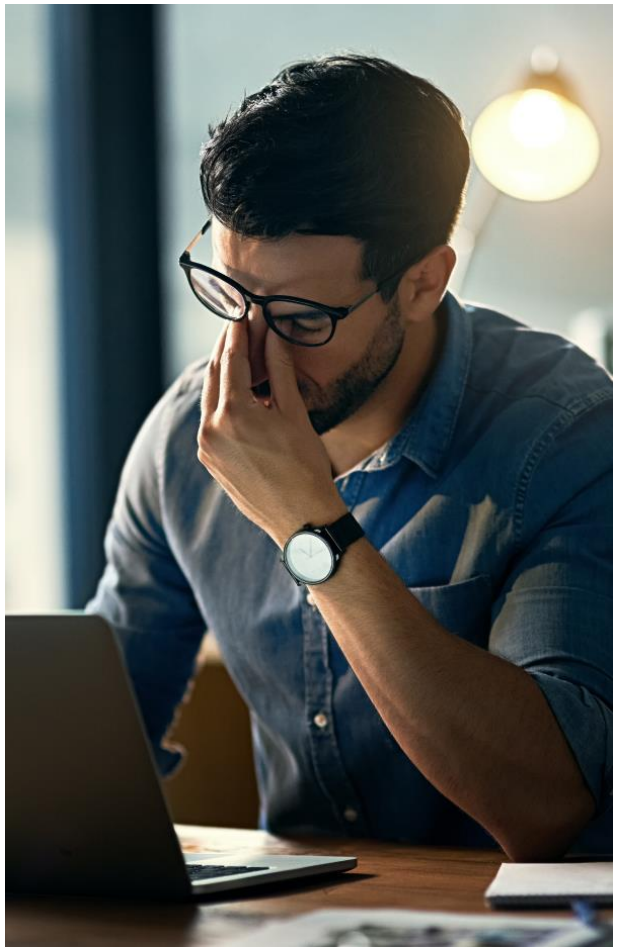
The Struggle is Real

In 2017, the FBI received more than 300,000 complaints with reported **losses of more than $1.4 billion dollars**.

The Mat-Su Borough in Alaska was declared a disaster zone – **$750,000 + in losses**.

More than just money, you also lose…

- Vital Services
- Valuable records, data, and intellectual property
- Productivity
- **Trust / Reputation**



“I am convinced that there are only two types of companies: those that have been hacked and those that will be.”

– Robert S. Mueller, III
Former Director FBI
March 1, 2012

Why Do Cyberattacks Happen?

- Bad actors will hack your data and demand immediate **payment**
- Selling **intelligence** is a giant industry
- Some hackers simply want **bragging rights** for shutting organizations down
- People want a **competitive advantage** by stealing your data
- Disgruntled employees and other bad actors may simply want **revenge**

Recent Attacks in Alaska

- Alaska Division of Health and Human Services – **500 personal records** (Zeus trojan)
- Fairbanks North Star Borough – **44,000 records compromised** through 3rd party billing
- City of Valdez – Police Department/City **offline for almost a week**
- Mat-Su Borough – hit by a **3-prong attack**:
  - Infected with a virus (Emotet)
  - Deployed a trojan (Bitpayment)
  - Installed malware (Dridex)

What's the Difference?

Virus. A contagious piece of code that infects the other software on the host system and spreads itself once it is run. It is mostly known to spread when software is shared between computers. This acts more like a parasite.

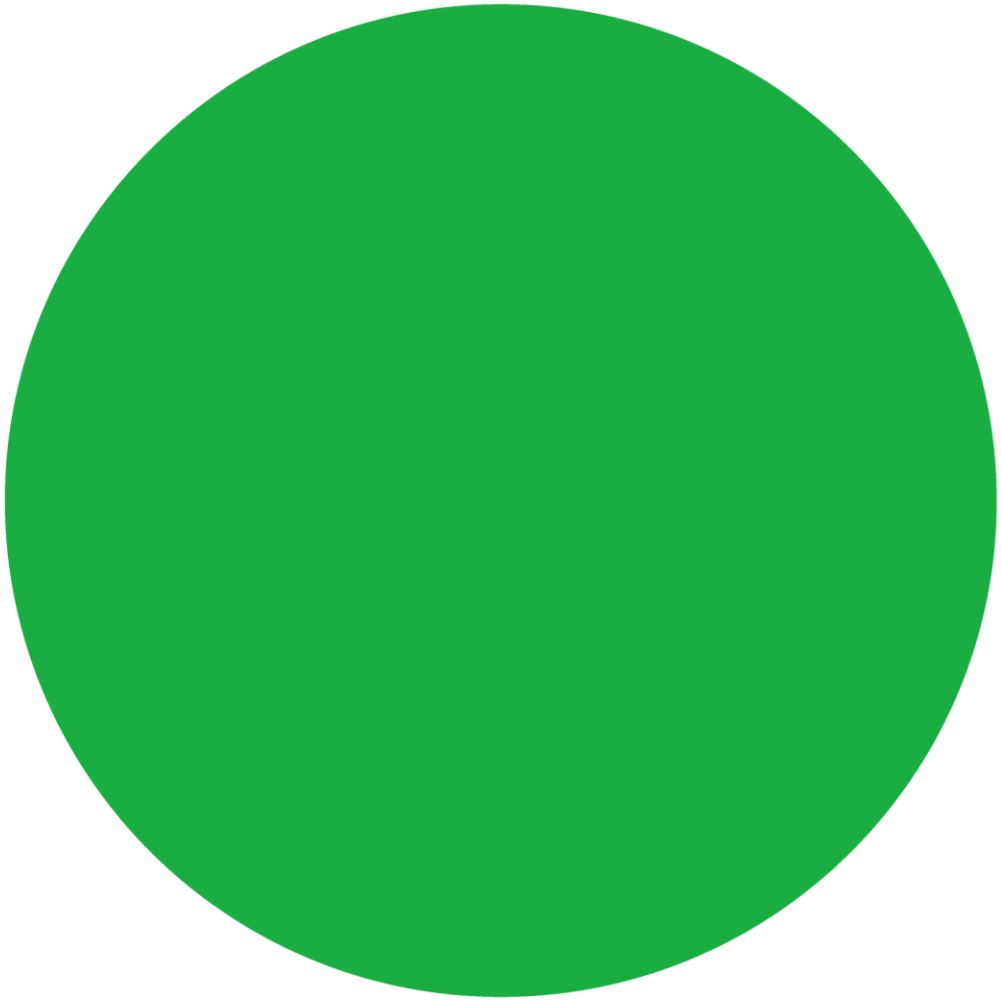
Trojan. A virus designed to make a user think they are a safe program and run them. They may be programmed to steal personal and financial information.

Ransomware. This is an advanced type of malware that restricts access to the computer system until the user pays a fee.

7 Layers of Protection

1. Backup

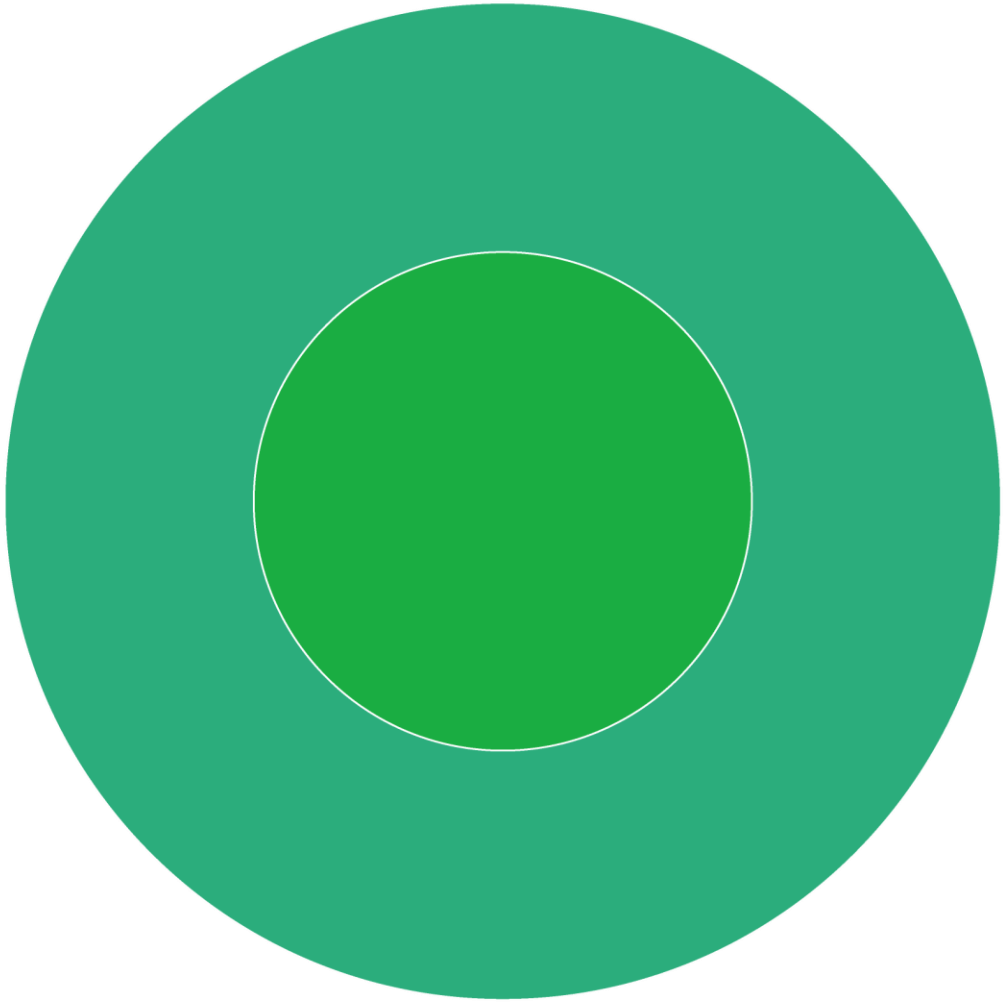
- Endpoint
- Servers
- Cloud



7 Layers of Protection

1. Backup
- Endpoint
- Servers
- Cloud

2. Data Security
- Data Encryption
- Identity & Access Management
- Public Key Infrastructure

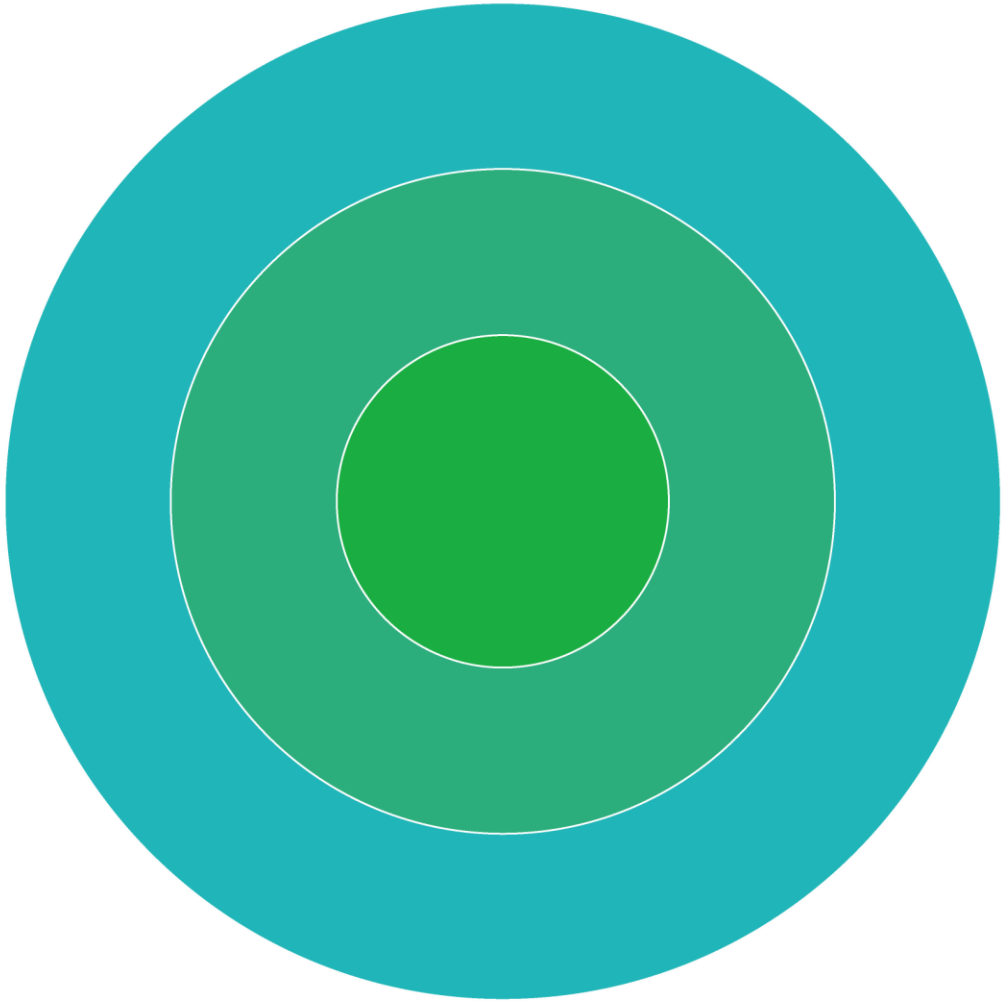


7 Layers of Protection

1. Backup
- Endpoint
- Servers
- Cloud

2. Data Security
- Data Encryption
- Identity & Access Management
- Public Key Infrastructure

3. Endpoint Security
- Antivirus/Antimalware (AV/AM)
- Patching
- Data Loss Prevention (DLP)



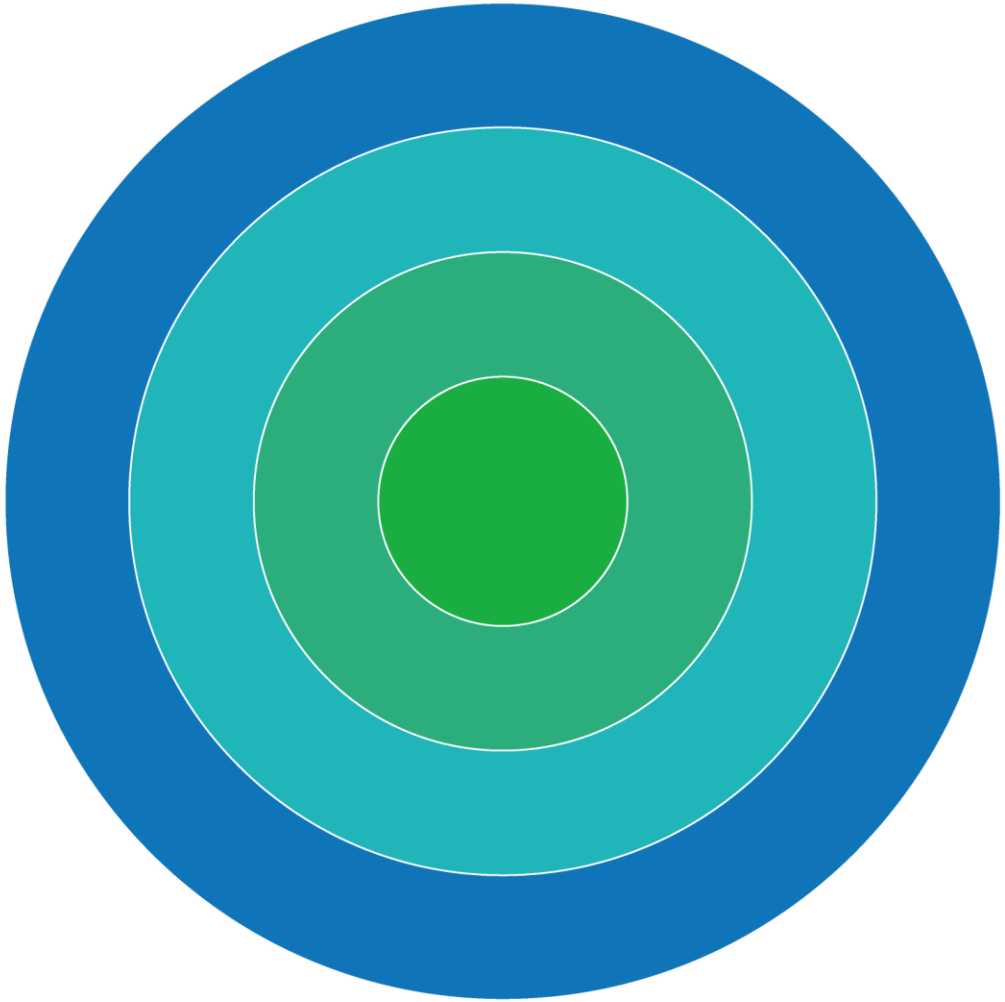
7 Layers of Protection

1. Backup
- Endpoint
- Servers
- Cloud

2. Data Security
- Data Encryption
- Identity & Access Management
- Public Key Infrastructure

3. Endpoint Security
- Antivirus/Antimalware (AV/AM)
- Patching
- Data Loss Prevention (DLP)

4. Network Security
- Enterprise-Level Intrusion, Detection, and Prevention Systems (IDPS)
- Enterprise Wireless Security
- VPN



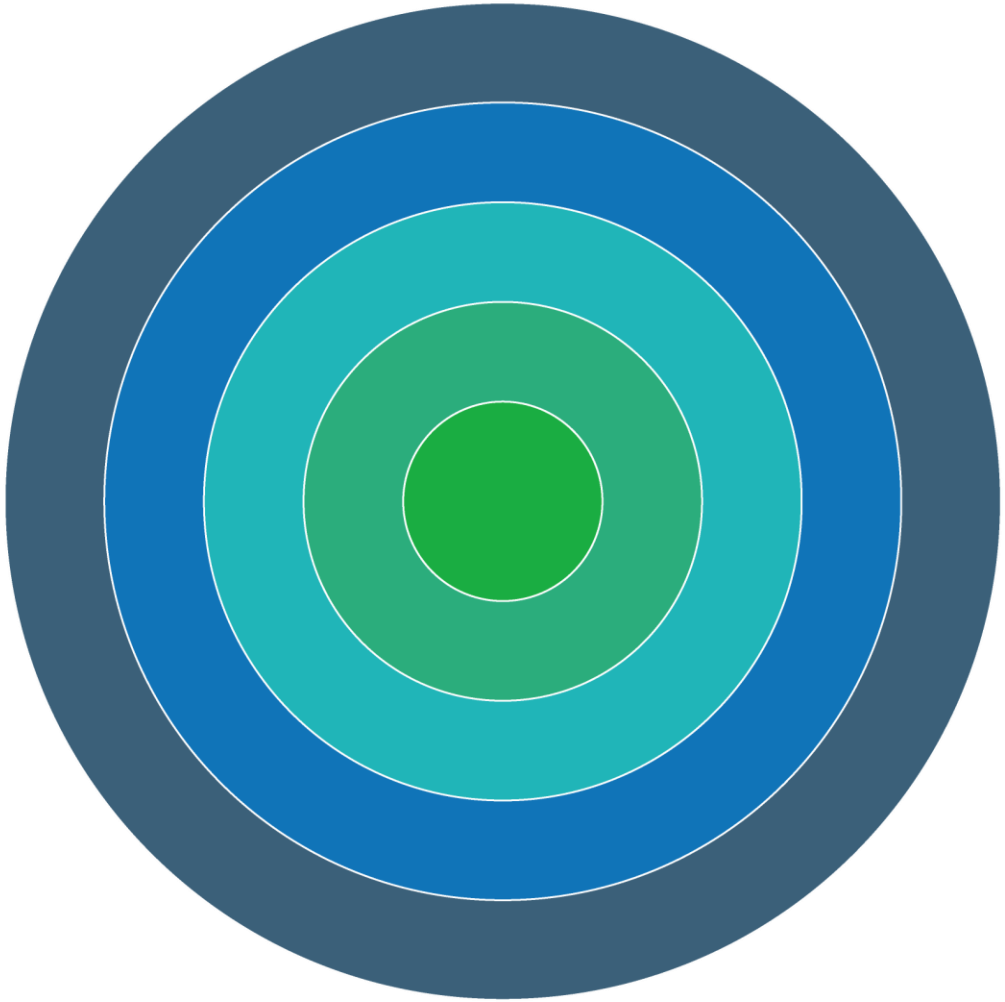
7 Layers of Protection

1. Backup
- Endpoint
- Servers
- Cloud

2. Data Security
- Data Encryption
- Identity & Access Management
- Public Key Infrastructure

3. Endpoint Security
- Antivirus/Antimalware (AV/AM)
- Patching
- Data Loss Prevention (DLP)

4. Network Security
- Enterprise-Level Intrusion, Detection, and Prevention Systems (IDPS)
- Enterprise Wireless Security
- VPN



5. Perimeter Security
- Internet Rules
- Secure DMZ

7 Layers of Protection

1. Backup
- Endpoint
- Servers
- Cloud

2. Data Security
- Data Encryption
- Identity & Access Management
- Public Key Infrastructure

3. Endpoint Security
- Antivirus/Antimalware (AV/AM)
- Patching
- Data Loss Prevention (DLP)

4. Network Security
- Enterprise-Level Intrusion, Detection, and Prevention Systems (IDPS)
- Enterprise Wireless Security
- VPN

5. Perimeter Security
- Internet Rules
- Secure DMZ

6. Policies *(Spans across all layers)*
- External Security Assessment
- Phish Testing
- Acceptable Use Practices
- Password Changes
- External Storage

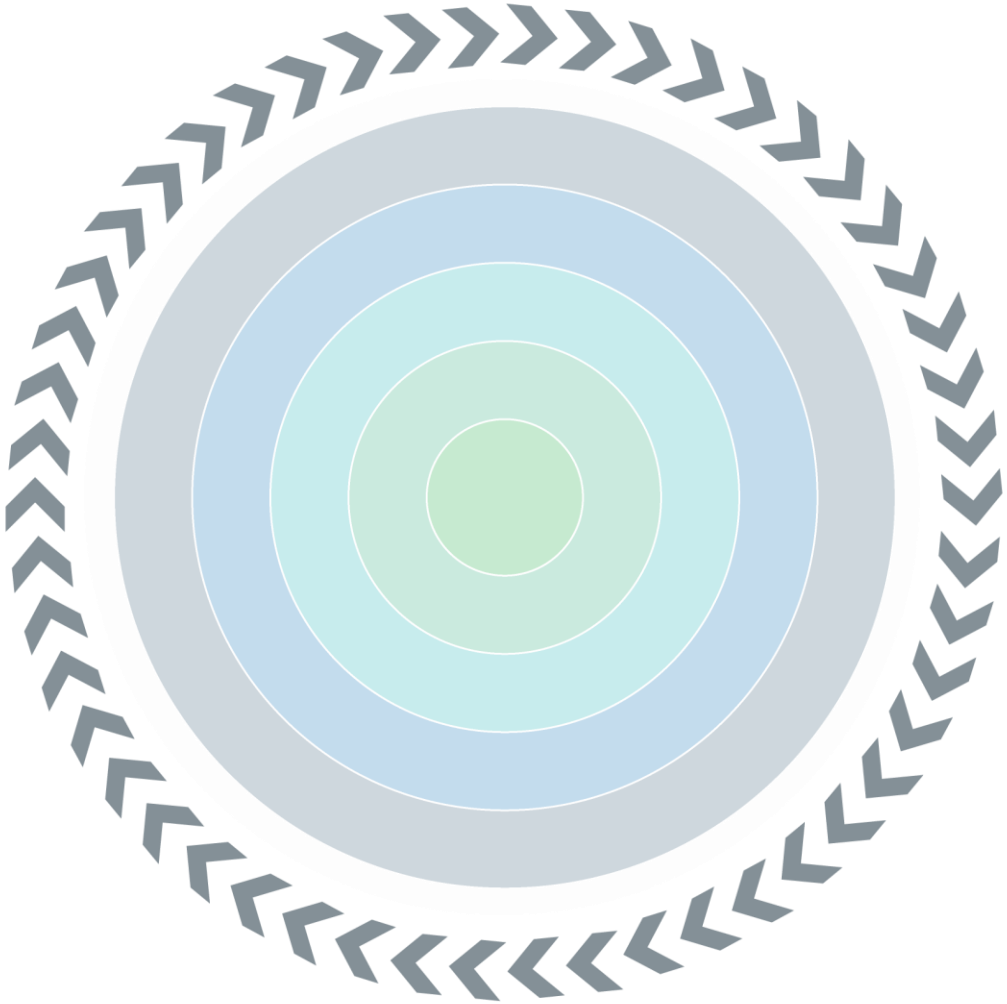
7 Layers of Protection

1. Backup
- Endpoint
- Servers
- Cloud

2. Data Security
- Data Encryption
- Identity & Access Management
- Public Key Infrastructure

3. Endpoint Security
- Antivirus/Antimalware (AV/AM)
- Patching
- Data Loss Prevention (DLP)

4. Network Security
- Enterprise-Level Intrusion, Detection, and Prevention Systems (IDPS)
- Enterprise Wireless Security
- VPN



5. Perimeter Security
- Internet Rules
- Secure DMZ

6. Policies *(Spans across all layers)*
- External Security Assessment
- Phish Testing
- Acceptable Use Practices
- Password Changes
- External Storage

7. Operations
- Continuous Monitoring
- Network Operations Center (NOC)
- Cyber Insurance

When It Does Go Wrong…

1. Isolate the System(s) If You Can
2. DO NOT Power the System Off
3. Contact Help
   - IT Support
   - FBI Cyber Incident Response – Nearest Field Office
   - Cyber Insurance Carrier

Contact Info for the Authorities

FBI Anchorage Field Office
anchorage.FBI.gov
(907) 276-4441

Internet Crime Complaint Center
www.ic3.gov

National Cyber Investigative Joint Task Force
24/7 CyWatch Command Center
(855) 292-3937
cywatch@ic.fbi.gov

The Best Defense…in This Case is a Strong Defense

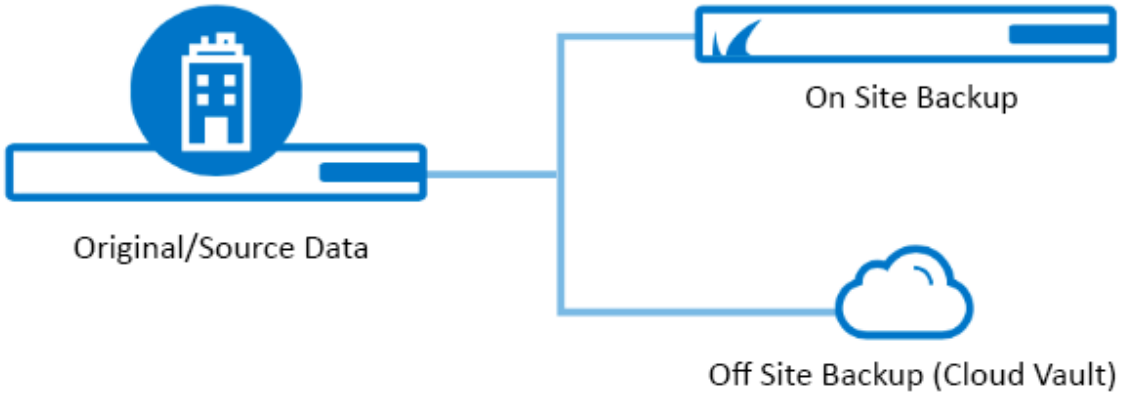
- Backups are key to defending your organization
- Paying the ransom does not guarantee your data will be restored
- Network shared folders do not suffice
- A “time machine” approach is best
- The time between backups is all you lose

Backing Up Your Data – Offline and Offsite

3 - 2 - 1

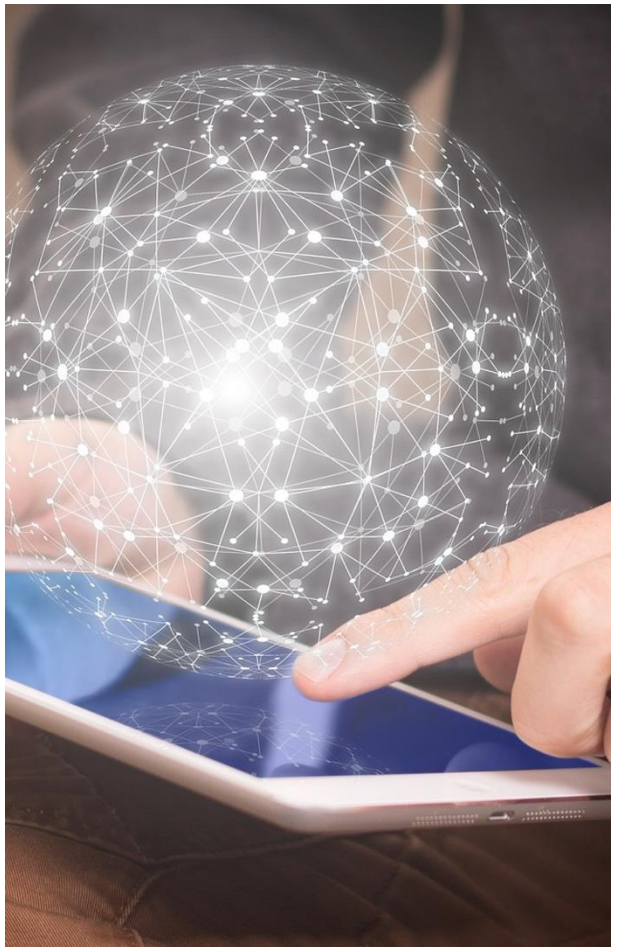
Follow the 3-2-1 rule:

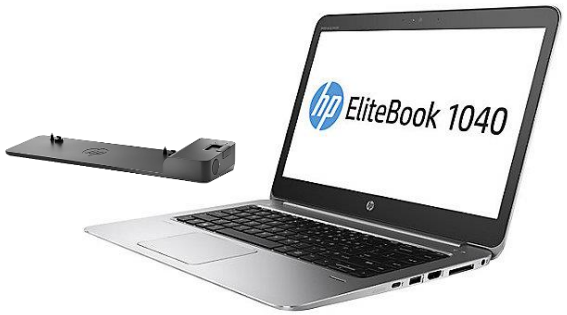
- **3** copies of your data
- Store it in at **2** different location
- **1** copy must be offsite



Best Backup Practices

- Data and system backup with both local and cloud vaults
- Fast recovery to minimize downtime
- Unlimited cloud storage; great for data archiving
- Simple management for single or multi-site deployments
- Solutions may be purchased (CapEx) or subscribed to (OpEx) for a lower fixed-price, monthly subscription





Use Current Equipment

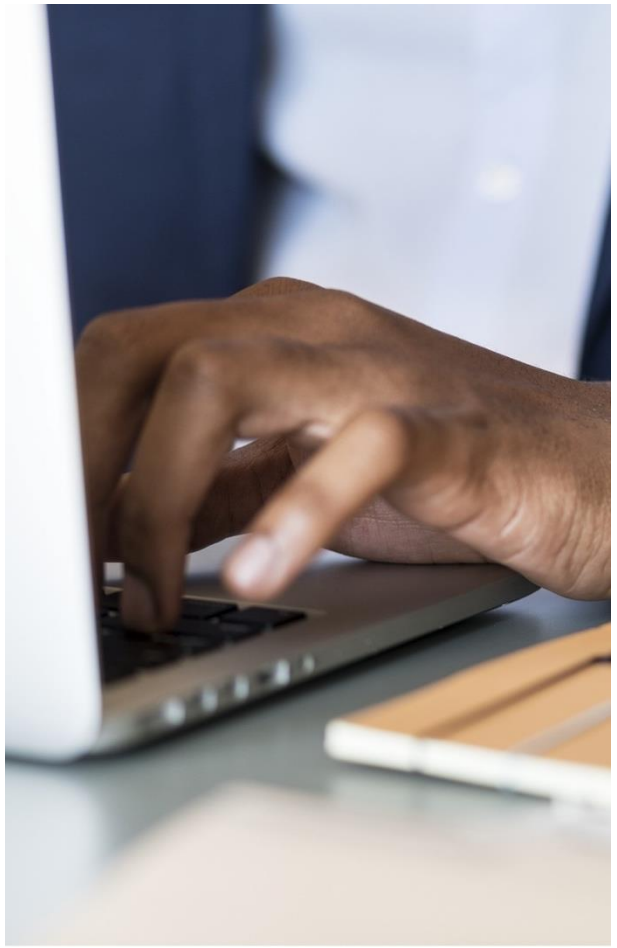
Subscribe to Hardware: Hardware as a Service Options

"HaaS" moves costs from CapEx to OpEx

- **New equipment.** Desktops, laptops, tablets, and networking components for low monthly payments
- **Easier on the cash flow.** Move your hardware purchases from your capital budget to your operating budget
- **Reliability assurance.** If equipment fails, it will be replaced hassle-free
- **Upgrades.** After the initial agreement is completed, you get to upgrade your devices every three years

The Importance of System Updates

- Ensures computers and software are fully-patched to reduce security risk
  - Many attacks leverage old exploits (e.g. Emotet, WannaCry, and WannaCrypt)
- Keep systems running at optimal efficiency – maximize employee productivity
- Best practices
  - Monitoring & Reporting
  - Automated/managed updates and patches
- Often included with Managed Services offerings that includes access to technical support for users



Thank You

Andres Gonzalez
agonzalez@arcticit.com
907-261-9538

ARCTIC IT
Tenacious Ingenuity™

Government Tribal Commercial