Behavioral Cybersecurity

THE PEOPLE SIDE OF COMPLIANCE

WITH DFAR 252-204-7012 & NIST SP 800-171

Digital Forensics

Computer systems have become a tool for committing various crimes.

Who Am I?

- Military Brat
- Behavioral and OCM Expert
- Your Work Dr™ (Organizational Psychology with Government – Fed (Homeland Security, FAA, VA), Tribal Nations, Educational Associations
- Currently working for City of Chicago

CyberSecurity

If you want people to do something, remove obstacles!

Every organization is responsible for ensuring cyber security. The ability to protect its information systems from impairment, or even theft, is essential to success. Implementing effective security measures will not only offer liability protection; it will also increase efficiency and productivity.

FACT:

95% of cybersecurity breaches in the last year were due to a human element

BEHAVIORAL CYBERSECURITY

Defense is Offense

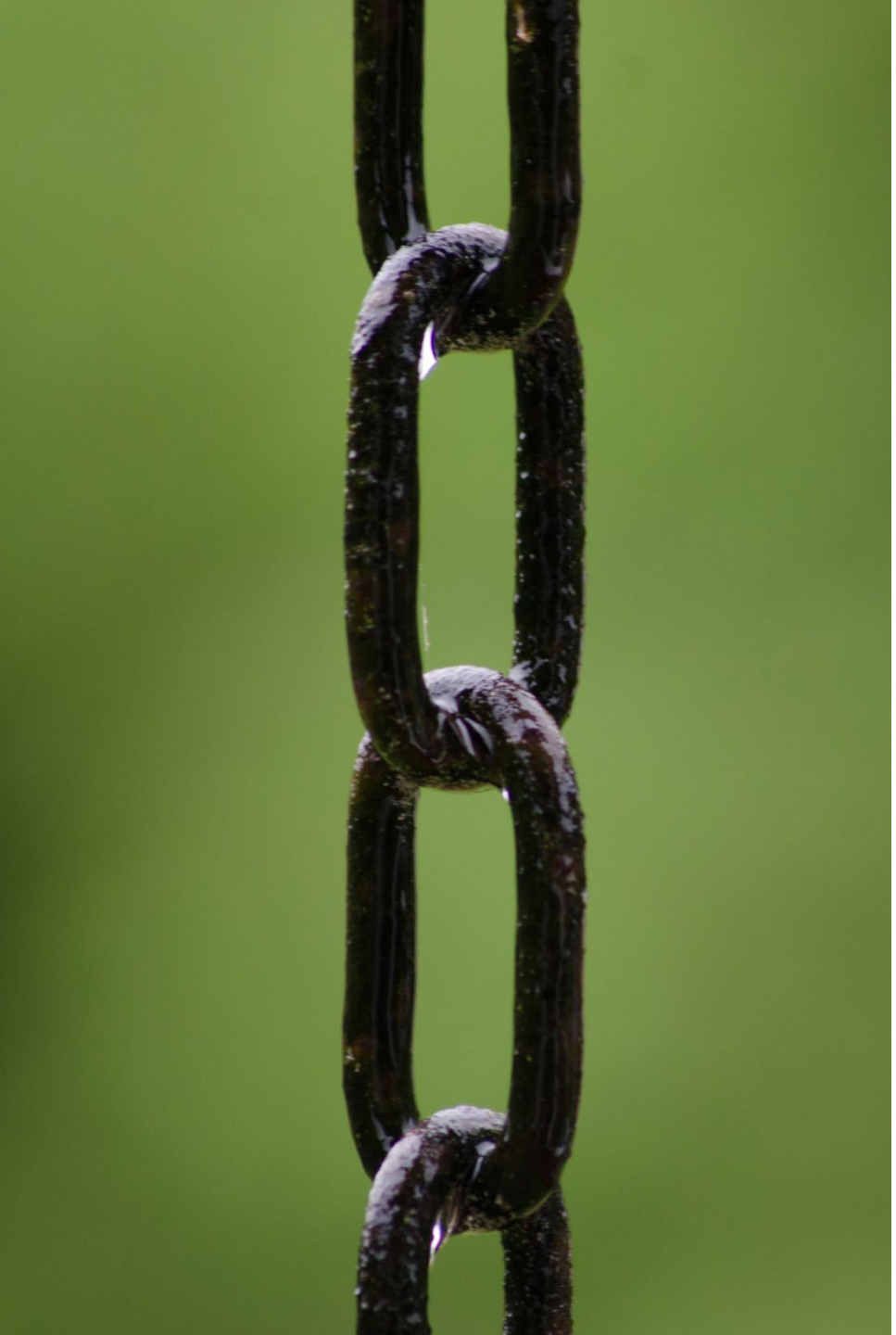
“The best defense is a good offense”. Rather than reacting to attacks once they’ve occurred, a wise strategy is to prepare proactive measures, so that if the time comes, you can completely bypass the attack, or lessen the blow of it.

Workshop Objectives

- Understand compliance with DFARDFAR 252-204-7012 & NIST SP 800-171 is not optional, possible consequences of non-compliance
- Know the types of cyber-attacks to look out for
- Develop effective prevention methods that recognize the people side of compliance

DFAR 252.204-7012 Compliance

- Understand compliance with DFAR 252-204-7012 & NIST SP 800-171 is **not optional** (since December 2017) **GLOBALLY**
- Compliance for **ALL contractors** is being vigorously enforced, possible consequences (ex. 300 contractors investigated- **75% WERE NOT** in-compliance)
- DoD Assessment, Cybersecurity Maturity Model Certificate
- Basic Safeguarding of Covered Contractor Information Systems



COMPLIANCE STEPS

- 1.1 NIST SP 800-171 Self Assessment (you MUST develop a plan and budget to fix the weaknesses. HIRE PROFESSIONALS to help
- 1.2 Plan of Action and Milestones (POAMS)
- System Security Plan
- Incident Response Plan and Reporting
- Subcontractor Flow Down Requirements

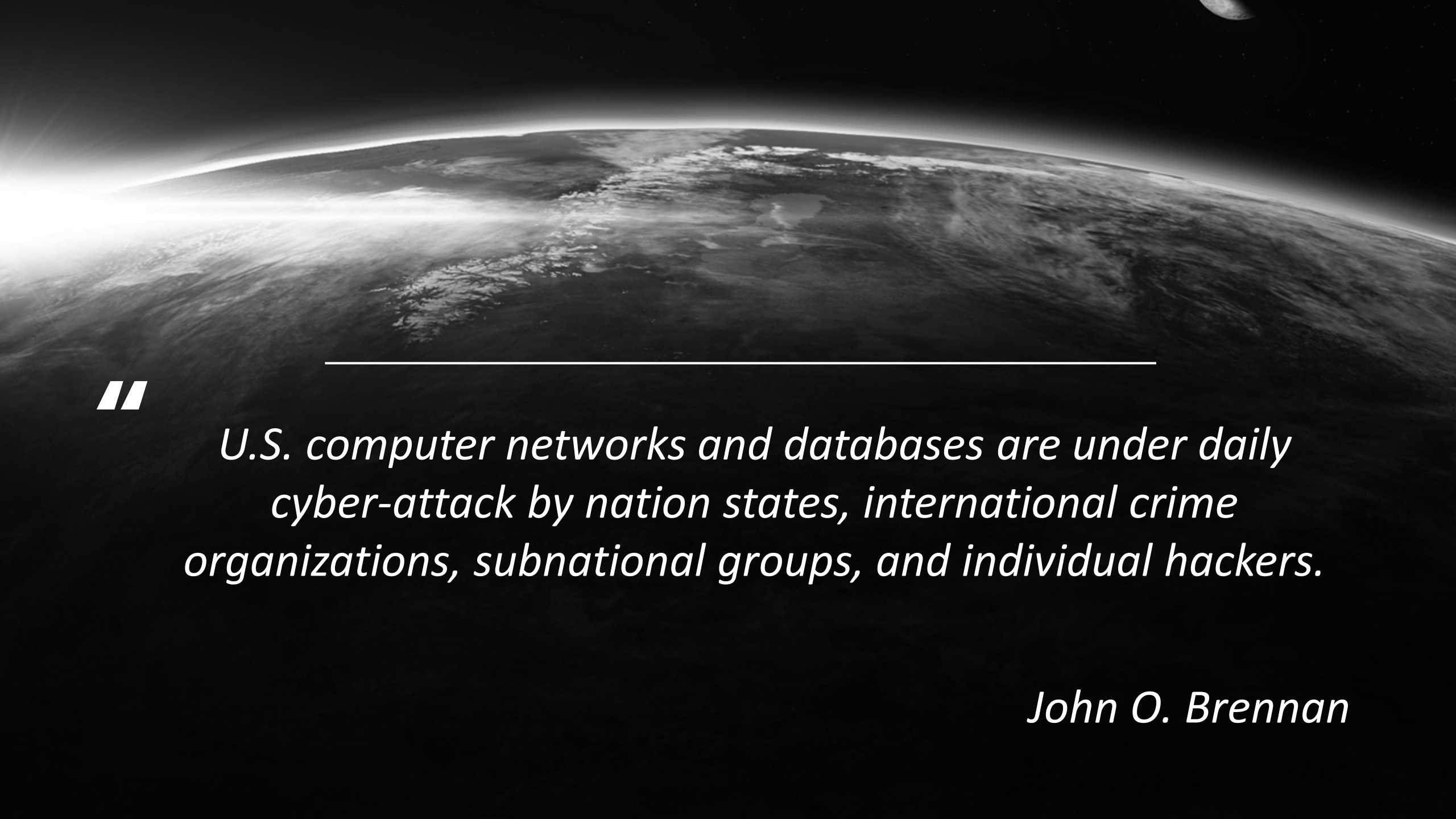
Need to know:

International Data Encryption Method (IDEA); Advanced Encryption Standard (AES); Data Encryption Standard (DES)

"The weakest link in any computer security system is PEOPLE. Unlike technology and processes people are complex. They think for themselves and make their own decisions. Sometimes those decisions are good decisions and other times they are bad ones. People are fallible and make mistakes. BIG ONES."

Know Your IoB's & BAU's

- **IOB's** = Traits or behaviors employers and managers use to assess the competency/key abilities of its employees
- **BAU's** = Business as usual work carried out by teams and individuals as part of their standard daily work practices and are the first to see which processes are working and what requires changing (inchstones)
- **Anytime a document** is created, saved, changed, mailed, shared, uploaded, downloaded, or deleted that documents context and intent is KNOWN
- **Train and reinforce** CyberSafe Behaviors Consistently and Constantly



"U.S. computer networks and databases are under daily cyber-attack by nation states, international crime organizations, subnational groups, and individual hackers.

John O. Brennan

BEHAVIORAL CYBERSECURITY

Critical Cyber Threats

Critical cyber threats are those that if carried out, could have a debilitating effect on an organization, or even a country.

Critical Cyber Threats

- Government facilities –
  Contractors, especially small business
- Finance
- Healthcare
- Communication Systems
- Dams

Cyber Espionage

The purpose of cyber espionage is to obtain the secrets of another, without their permission.

Legal Recourse

- Obtaining National Security Information
- Accessing a Computer and Obtaining Information
- Trespassing in a Government Computer

BEHAVIORAL CYBERSECURITY

Cyber Security Fundamentals

Before developing and implementing security measures to comply with DFAR 252.204-7012 and prevent cyberattacks, **you must understand basic concepts associated with cyber security and what cyberattacks are.**

What are parts of the CyberDomain?

- The Physical Domain
- The Logical Domain
- The Data Domain
- The Application and User Domain

What is Cyber Security?

The implementation of methods to prevent attacks on a company's information systems, to secure Personally Identifiable Information (PII).

Why is Behavioral Cybersecurity?

- Focuses On Heuristics
- Detects Anamolies
- A Proactive Approach To Stopping Cyber Threats

What is a Hacker?

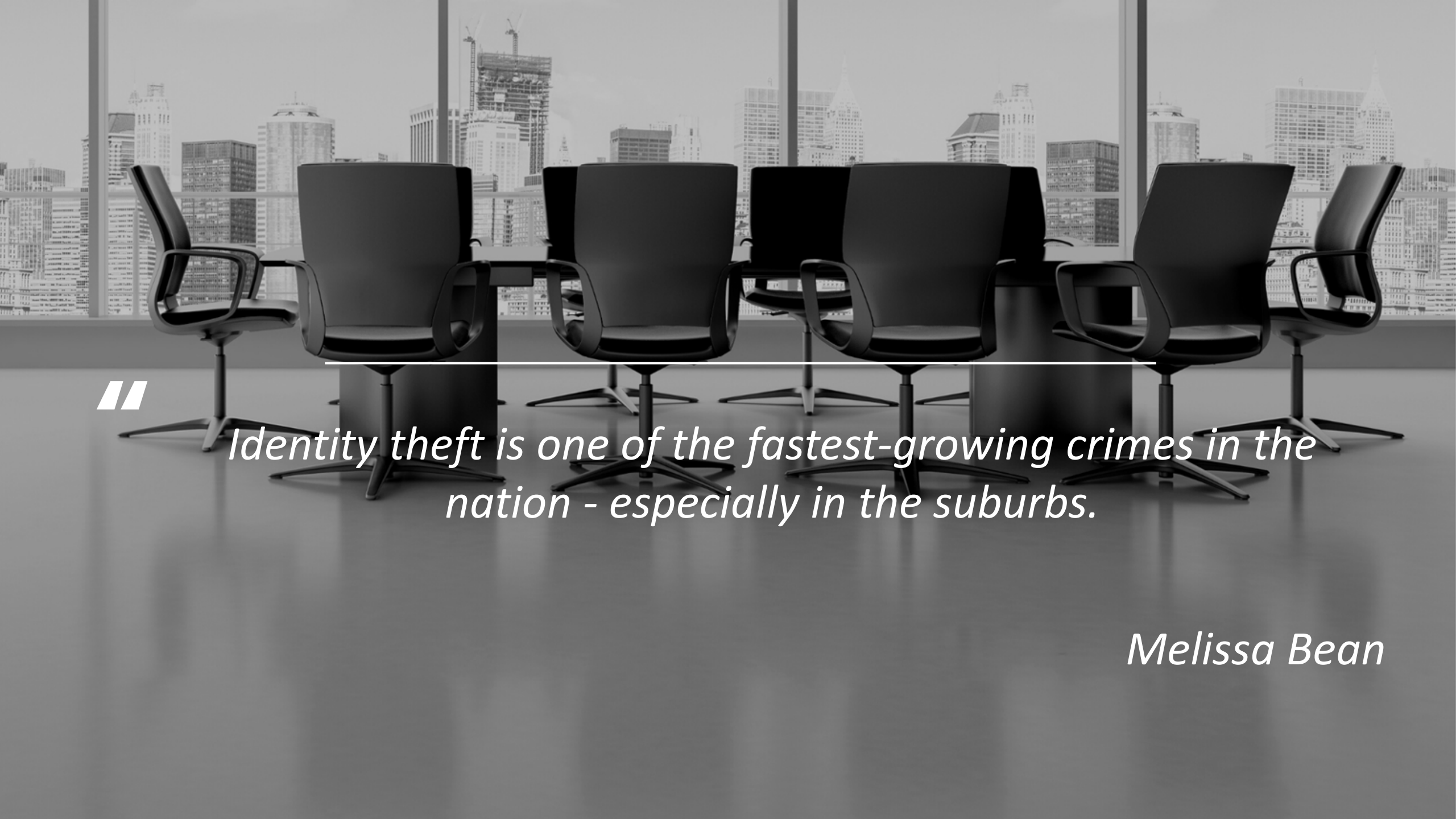
- Grey hats: do it “for the fun of it”.
- Black hats: stealing and/or selling data for monetary gain.

Cyber Terrorism

Cyber terrorism is cyber threats/attacks on a large scale.

Practical Illustration

- What is Cyberspace?
- What is Cyber Security?
- Why is Behavioral CyberSecurity Important?
- What is the percentage of data breaches due to the human element?

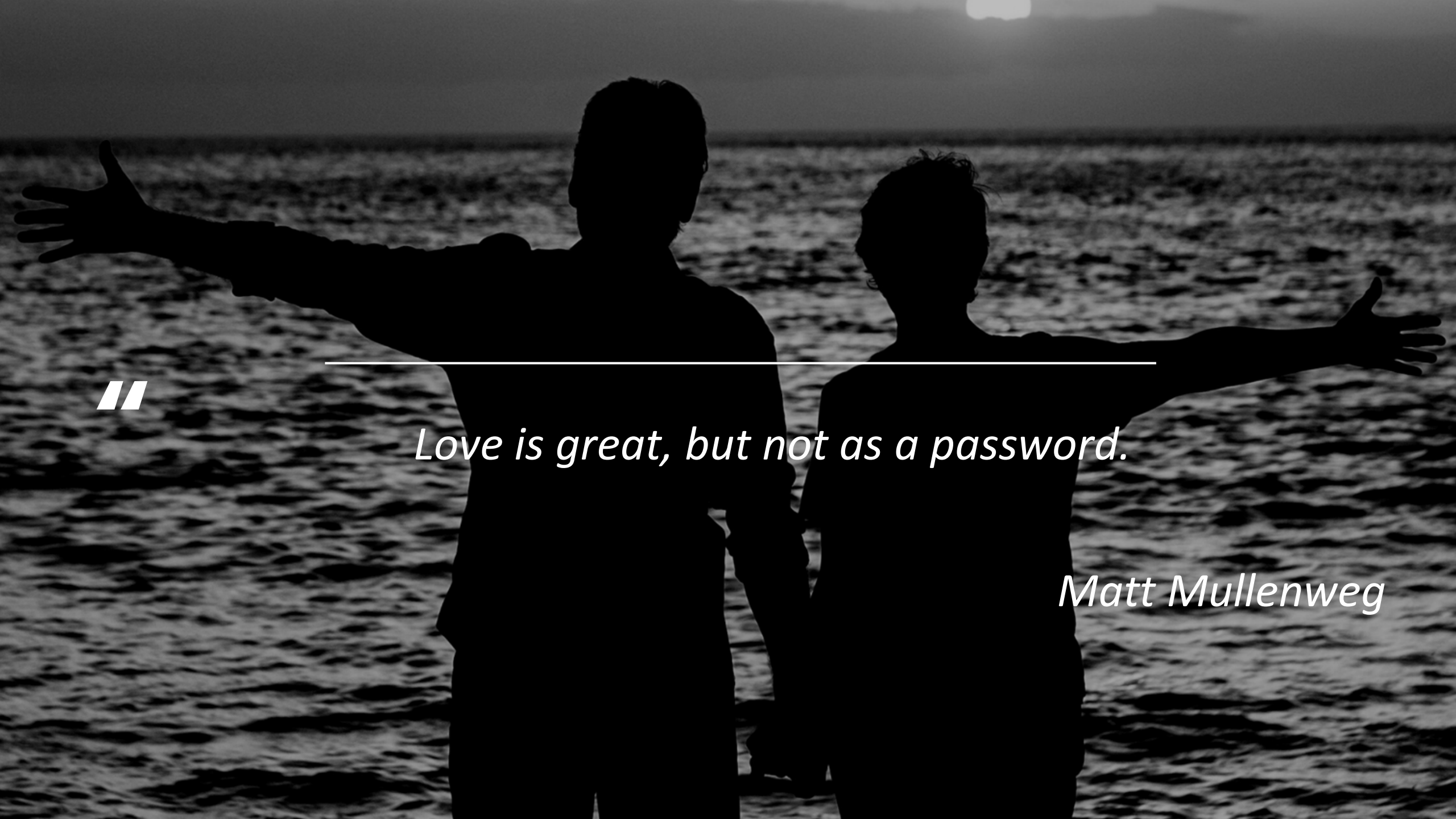


"Identity theft is one of the fastest-growing crimes in the nation - especially in the suburbs.

Melissa Bean

Identity Theft

- Be mindful of phishing websites
- Utilize an Anti-virus / Anti-malware program
- Don’t respond to unsolicited requests



Love is great, but not as a password.

Matt Mullenweg

Craft a Strong Password

Avoid using common words or consecutive characters to make up your password (e.g., Do not use “password” as your password. Do not use a password such as Office111).

Passwords Attacks

- Include upper- and lower-case letters, numbers, and symbols
- Craft a password that is long
- Regularly update your password

Don’t Save Passwords

- Treat them as you would other important documents by locking them in a safe or drawer that requires a key
- Invest in a password manager service

Two- Step Verification

- Token
- Key
- Password
- Pin
- Fingerprint
- Voice recognition

Place Lock on Phone

Avoid using common words or consecutive characters to make up your password.

Practical Illustration

- Craft a Strong Password
- Two-Step Verification
- Download Attachments with Care
- Question Legitimacy of Websites

POLL

1. What is the best way to store a password?

A. On a sticky note, on your desk

B. In your memory

C. In your phone

D. In a notebook located in an unlocked desk

Poll #2

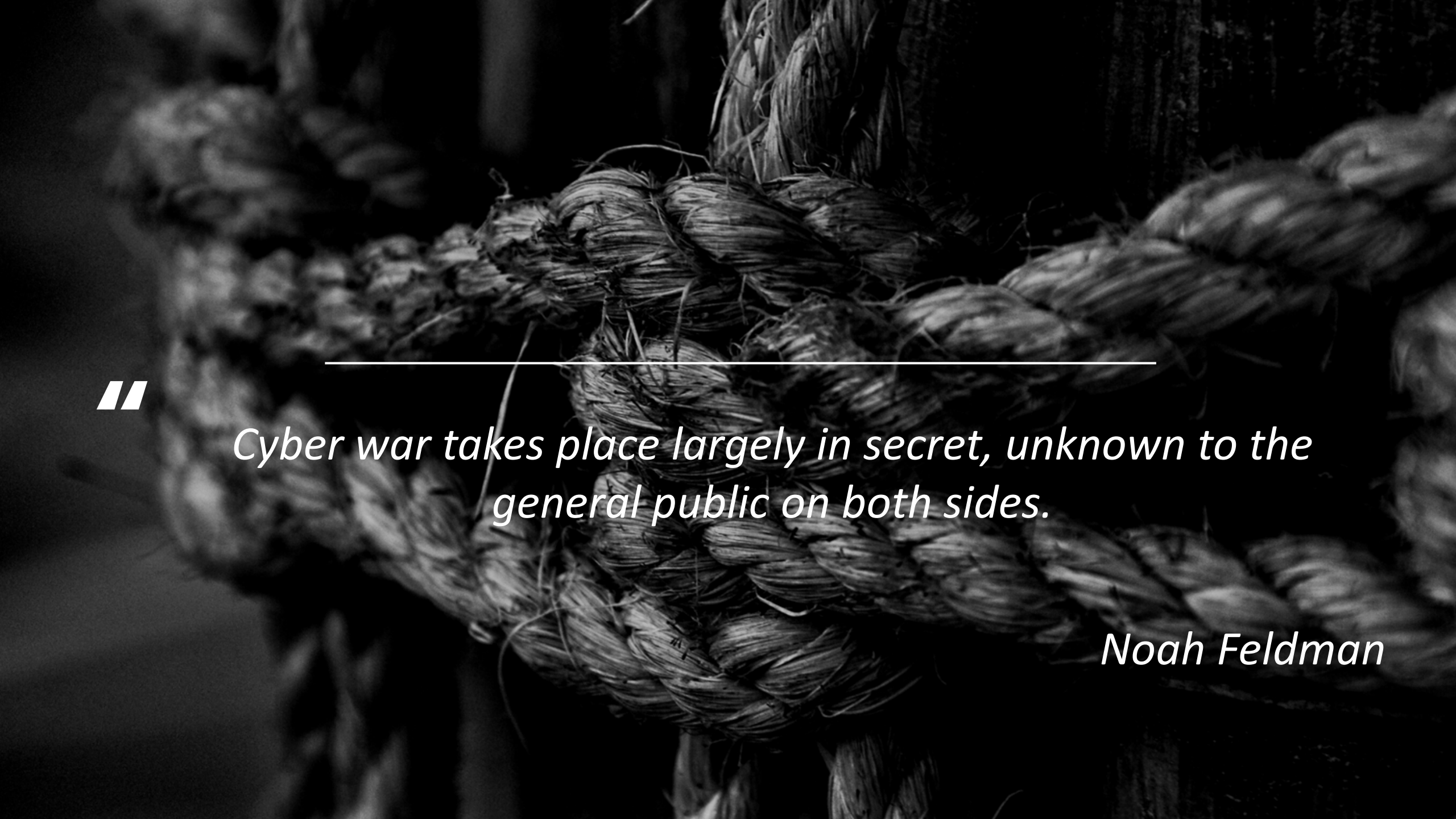
4. To create a strong password, it should have:

A. Letters and numbers

B. Numbers and symbols

C. Letters, numbers, and symbols

D. Letters and symbols



"Cyber war takes place largely in secret, unknown to the general public on both sides.

Noah Feldman

Viruses

- Corrupting files
- Computer slowdown
- Taking over basic functions of the operating system

Incident Response Planning

- Have a policy program in place
- Build trust with the government and your clients that you protect their data
- Mitigating any enterprise risk, testing practices to put plans into ACTION

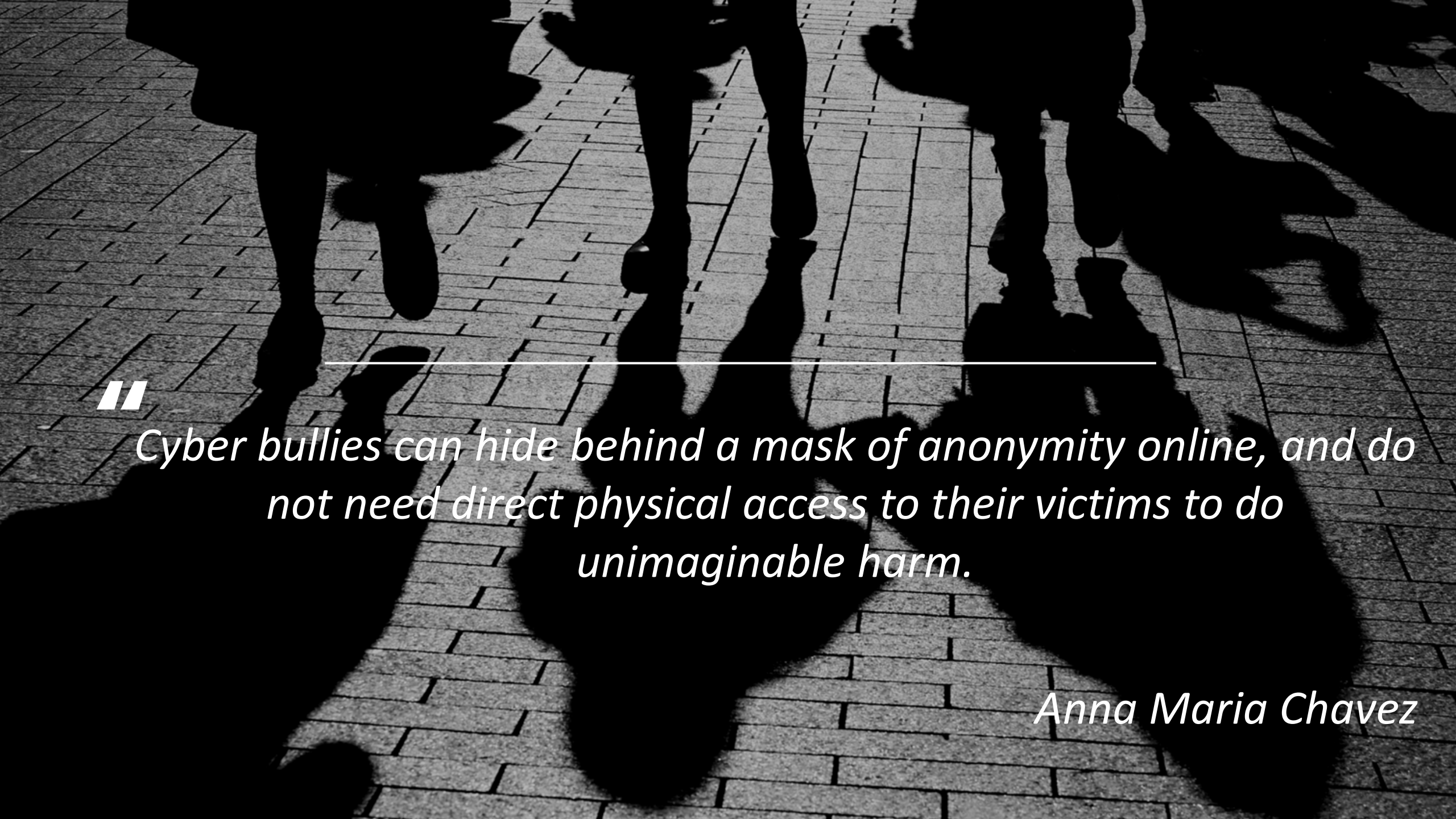
Today's Phishing Attacks

- Using Technology advancements defenders use to protect users (AI and Machine Learning)
- Increasingly narrowly targeted and crafted to subvert Collecting personal information
- Installing unsolicited software
- Redirecting web browsers

BEHAVIORAL CYBERSECURITY

Cyber Security Breaches

Whether the data is released intentionally or unintentionally, the consequences can have long-lasting effects, from harassment to identity theft.



"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm.

Anna Maria Chavez

Routine Updates

- High priority
- Suggested
- Drivers

NOT REGULARLY DONE BY OVER 60% OF COMPANIES/CONTRACTORS

Phishing

Cyber criminals who use phishing scams aim to obtain personal information by appearing to be a legitimate source.

Passive Attack

A passive attack is conducted to simply find the vulnerabilities of a system, but not change any data at that time.

Penetration Testing

- Determine the bearing an attack will have on a company
- Assess the company's network risk management capabilities

Harassment

- Do not immediately respond
- Tell the cyberbully to stop
- Get the authorities involved

Cyber Stalking

The cyber stalker’s intention is typically to intimidate, or in some way influence, the victim.

Cyber Warfare

Cyber warfare is a means of war against another state or country to damage that other state/country's information networks.

Denial of Service Attacks

- Network performs slowly
- A specific website is inaccessible
- No websites are accessible

Practical Illustration

- Phishing
- Identity Theft
- Harassment
- Cyber Stalking

BEHAVIORAL CYBERSECURITY

Social Network Security

Many people forget that with social networking, revealing too much information about oneself could still lead to dangerous situations, such as social engineering attacks.

Don’t Link Accounts

Linking social media accounts makes it easier for thieves to find you.

Have a Private Profile

- Facebook
- Instagram
- Twitter
- Google+
- LinkedIn
- Pinterest

Keep Birthdate Hidden

If you absolutely must list your birthdate, do not include the year.

Don’t Reveal Location

Use randomized IOP to make a fake location or input a city/state different from where you are located.

BEHAVIORAL CYBERSECURITY

Steps You Must Take NOW

It may not be possible to completely avoid falling victim to cybercrime.

Having a tool kit of prevention methods could help your organization minimize the risk of cyber crimes.

CHANGE- create a budget, hire professionals for assessments and perform Change Management for every part of your organization AND YOURSELF

Words From the Wise

Everybody should want to make sure that we have the cyber tools necessary to investigate cyber-crimes, and to be prepared to defend against them and to bring people to justice who commit it.

- Janet Reno

Somebody could send you an office document or a PDF file, and as soon as you open it, it's a booby trap and the hacker has complete control of your computer.

- Matt Gentile

People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical.

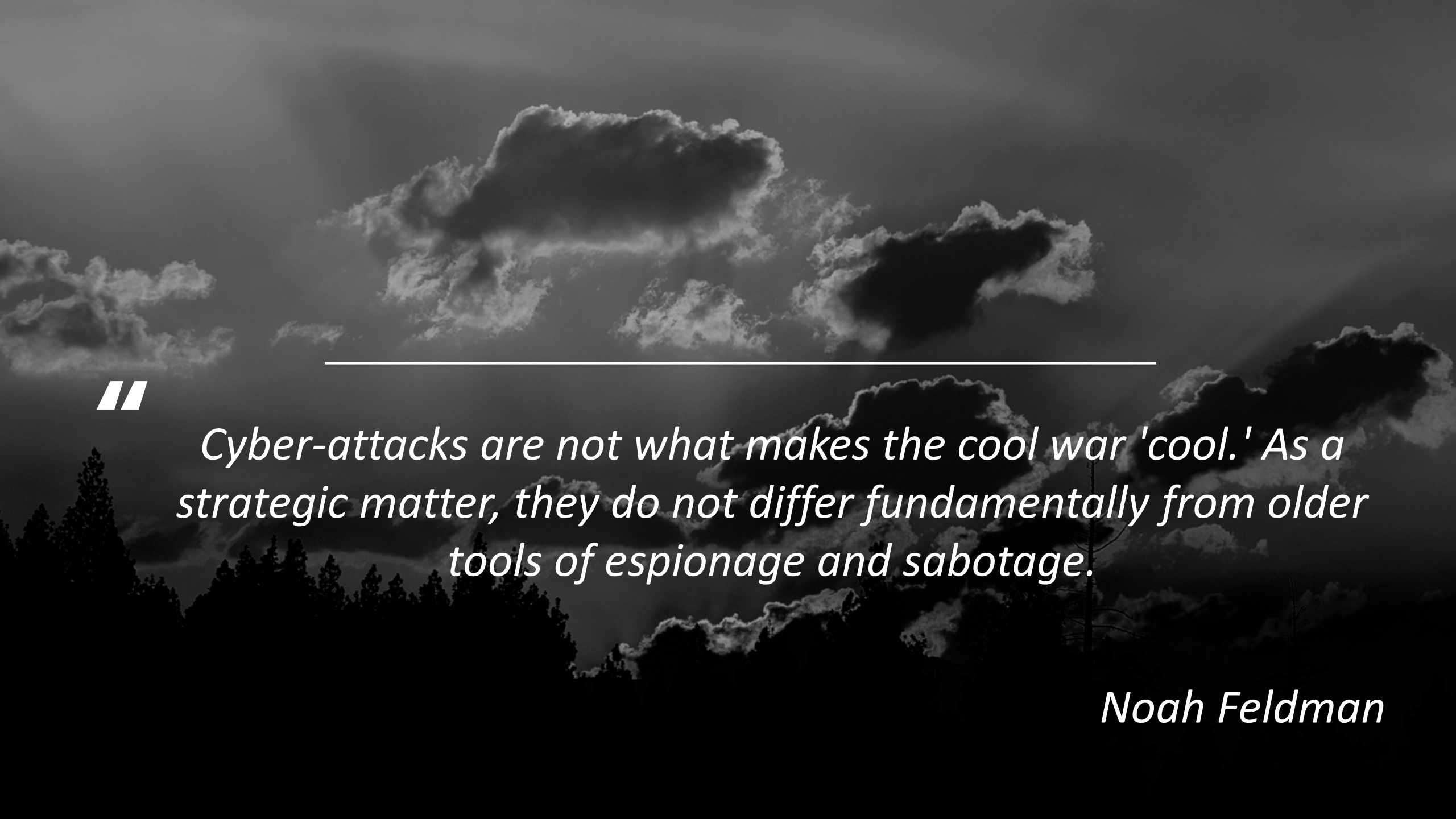
- Frank Abagnale

Questions?

Assessment and Referral Contact Information:

clientexp@dr-cheryl.com

469-403-4778



"Cyber-attacks are not what makes the cool war 'cool.' As a strategic matter, they do not differ fundamentally from older tools of espionage and sabotage.

Noah Feldman