Reducing Your Cyber Risk Exposure

John Giantsidis, JD, M.Eng.

President

CyberActa, Inc.

Webinar – Sponsored by The Florida Bar Board Technology Committee & LegalFuel – Thursday, January 12, 2023

John Giantsidis, JD, M.Eng.

- Empowering clients with cybersecurity, privacy, data, regulatory compliance, and commercialization solutions.
- US Marine Corp Cyber Auxiliary (Cyber Aux).
- Cybersecurity & Infrastructure Security Agency (“CISA”), Healthcare PoC Member.
- Vice Chair, The Florida Bar Technology Committee.
  - FL Bar Member since 2007
- Founding Member, Center for Healthcare Information Security, Inc.
- Advisor, Software Transparency Group, US Dept of Commerce, National Telecommunications and Information Administration.
- Past Voting Member, AAMI® Health IT Committee & Device Security Working Group.

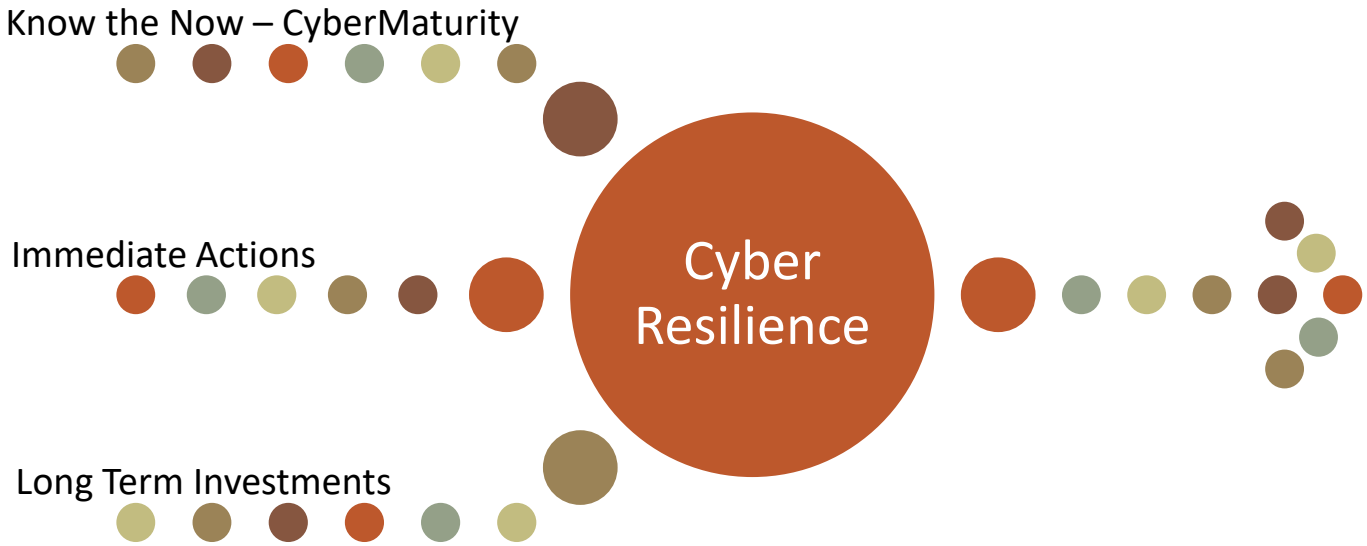
The rate of technology change and adoption has easily outpaced most firms' ability to manage the associated risks. These include risks to intellectual property, client data and sensitive internal data. Cyber resilience enables firms to minimize disruption and continue to function in the event of a disruptive incident.

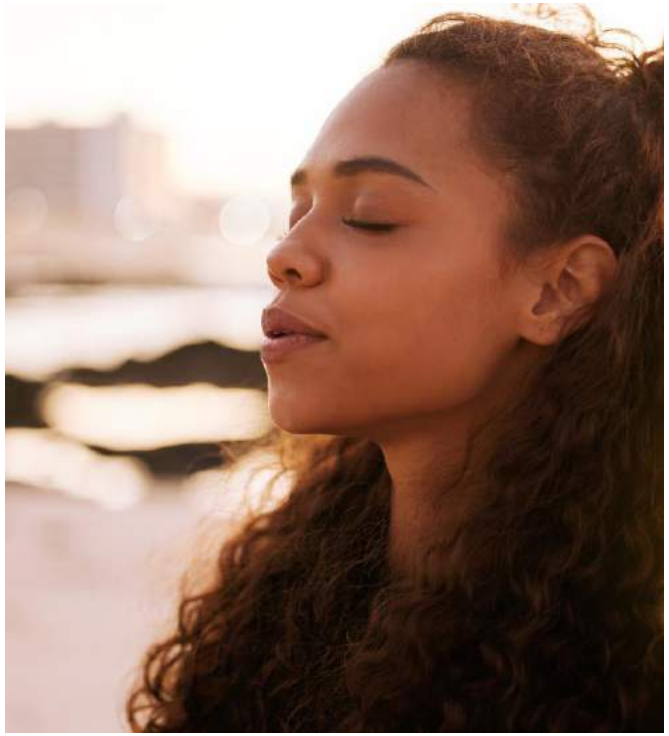
NOW MORE THAN EVER, FIRMS NEED TO HAVE PROVEN STRATEGIES TO DEAL WITH DISRUPTIVE CYBER EVENTS, UNDERSTAND RISKS AND BE BETTER PREPARED TO FACE THESE CHALLENGES – A FRAMEWORK OF 'CYBER RESILIENCE'.

Where do we start?

CYBER RESILIENCE STARTS WITH KNOWLEDGE.

Strategy to a cyber peace of mind





Cybersecurity Maturity Questionnaire

To help you determine your firm's level of cyber maturity, and to help you better integrate cybersecurity into your practices, here is a self-assessment questionnaire divided into two:

Section A. Organizational Questions (10 questions)

Section B. Technical Questions (10 questions)

For each question, choose the answer that you think best reflects the reality of your firm. Each answer is awarded points:

- Not sure (I do not know): Zero points.
- No: 1 point
- Yes, but the implementation leaves something to be desired: 2 points
- Yes, and implementation is effective: 3 points

Section A. Organization Questions

1. Does your firm have a team, or a point of contact dedicated to information security management?

- (0) Not sure/I do not know
- (1) No
- (2) Yes, but within the firm, few people know who/how to contact
- (3) Yes and within the firm, everyone knows where to turn

Section A. Organization Questions

2. Your firm probably handles personal data, but does it have a Data Protection Officer (DPO)?

- (0) Not sure/I do not know
- (1) No
- (2) Yes, but you do not know who it is
- (3) Yes, and you know how to contact

Section A. Organization Questions

3. Has your firm completed a risk analysis or data protection impact analysis in the last six months?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but you do not know the results
- (3) Yes, and you know the corrective measures that have since been implemented

Section A. Organization Questions

4. Does your firm have an information security policy for employees (internet, social media, mobile devices)?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but this policy is not known by all staff
- (3) Yes, and this policy is the subject of cybersecurity training/awareness for employees

Section A. Organization Questions

5. Does your firm have a security policy or guidelines regarding suppliers/vendors that can access certain (potentially) sensitive areas or information?

- (0) Not sure/I do not know
- (1) No
- (2) Yes, but it is not always easy to tell the difference.
- (3) Yes, and contracts with suppliers have specific clauses, identified as such and information circulates only according to the firm's data classification policy.

Section A. Organization Questions

6. Does your firm provide guidelines to its attorneys/employees regarding the processing and "classification" of sensitive information?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but these instructions are so complicated that no one applies them
- (3) Yes, and these instructions are understood and applied

Section A. Organization Questions

7. Does your firm have a business continuity plan (BCP) or disaster recovery plan (DRP) or incident response plan (IRP)?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes but no one knows them and/or these procedures have never been tested
- (3) Yes, staff know these procedures, and regular tests (at least once a year) are organized

Section A. Organization Questions

8. Does your firm give instructions to its employees on how to work securely when they are outside their usual work environment?'

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but there is no VPN
- (3) Yes, and access is protected by a private virtual network (VPN)

Section A. Organization Questions

9. Does your firm have a policy that includes choosing a strong password/passphrase and raising awareness about password protection?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but "strong" passwords are difficult to remember. Post-it notes are everywhere, passwords are exchanged between colleagues, the same passwords are constantly reused...
- (3) Yes, and everyone knows how to form a strong password, where to store it safely, and how to exchange information between colleagues without exchanging personal passwords.

Section A. Organization Questions

10. When introducing new clients/cases/projects, does your firm assess the impact on information security?

- (0) Not sure/I do not know
- (1) No
- (2) Yes, in principle but in fact... It's a different story.
- (3) Yes, every attorney/staff knows that they must include this item in the agenda and that no new client/case can come out without considering security and data protection

Section B. Technical Questions

11. Does your firm regularly organize backups of all its servers?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but these backups are never tested
- (3) Yes, and these backups are regularly tested

Section B. Technical Questions

12. Does your firm regularly maintain its systems (OS) and applications up to date?

- (0) Not sure/I do not know
- (1) No
- (2) Yes, but not automatically. Each staff member must update their OWN applications. It is difficult to know whether everyone has done it correctly
- (3) Yes. The OS is updated automatically, and applications are reviewed and tested after any changes to the operating systems

Section B. Technical Questions

13. Has your firm installed a firewall between your firms' computers and the internet?

- (0) Not sure/I do not know
- (1) No
- (2) Yes but no one knows if/how it works
- (3) Yes and qualified staff regularly analyze reports and take appropriate action, if necessary

Section B. Technical Questions

14. Does your firm have a spam or phishing filtering or blocking tool?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes but no one knows how to spot spam/phishing or how to react to this type of e-mail.
- (3) Yes, and staff is trained to recognize and react correctly to spam/phishing

Section B. Technical Questions

15. Does your firm use malware protection?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but not on all company computers
- (3) Yes, on all computers, and these tools are regularly updated

Section B. Technical Questions

16. Has your firm implemented access control?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but in practice, everyone ends up having access to everything
- (3) Yes, and not everyone has access to everything

Section B. Technical Questions

17. Does your firm use an encryption tool to protect sensitive information before transmitting it outside the firm (for example, in the case of sending attachments containing confidential/sensitive/personal information)?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes but no one knows how to use it
- (3) Yes, and staff have been trained to use it

Section B. Technical Questions

18. Has your firm implemented (continued) training on information security?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, they form in-house only and/or only upon arrival
- (3) Yes, and the staff members concerned are ongoing in-house and external training

Section B. Technical Questions

19. Does your firm secure its servers/cloud presence and network components efficiently?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but security logs on servers and firewalls are kept for only one month and no one has time to analyze them properly
- (3) Yes, and the security logs on servers and firewalls are kept for at least 6 months.

Section B. Technical Questions

20. Does your firm regularly have its information security assessed?

- (0) Not sure/I do not know.
- (1) No
- (2) Yes, but it does not require anything from its suppliers, and no one in-house assesses the usefulness of the information collected during the audits
- (3) Yes, and the usefulness of the information collected is also assessed whether the audit is internal or whether it is an audit on suppliers.

Cybersecurity Maturity Results

If you have completed the self-assessment questionnaire.

If your score is between **0 and 20**, consult with other people in your firm to start planning and installing the first cybersecurity measures. Do not be discouraged: focus on the short-term essentials.

If your result is between **20 and 40**, your firm has already made some efforts to improve its cybersecurity... but parts of your approach still need to improve upon.

If your score is between **40 and 60**, congratulations! Your firm has already made many advances in several areas of cybersecurity. But do not rest on your laurels: new threats are constantly emerging! Do not forget to conduct regular security audits and plan, depending on your needs, the next steps to improve yourself.

Immediate Actions

STEPS YOU CAN TAKE NOW TO IMPROVE YOUR CYBER RESILIENCE!

Immediate Actions

- Awareness
  - Be wary of messages about money, urgent & attachments.
- Turn on Automatic Updates
  - OS and Apps
- Turn on MFA
- Strong Passwords/Passphrases
- Apply Access Control
- Backups
- Encrypt

Awareness

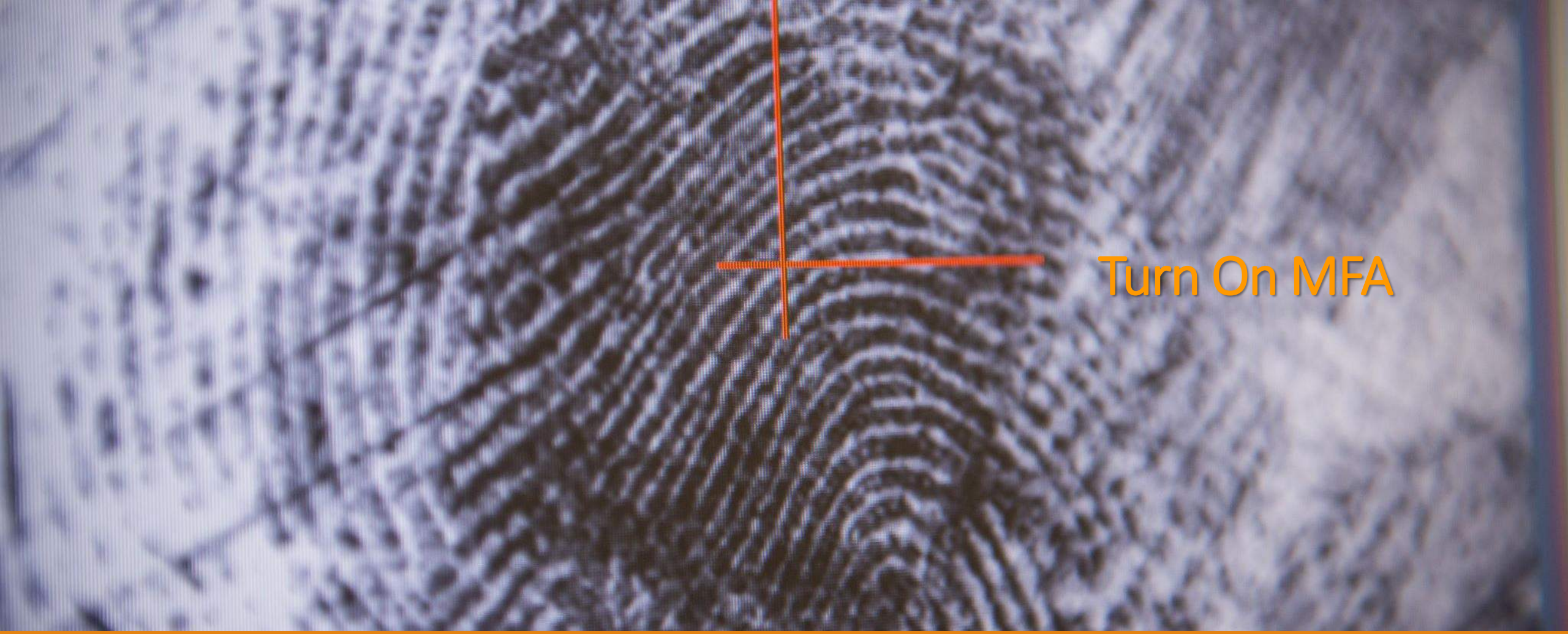
Be wary of all messages received by email, SMS, instant messaging apps or social networks:

- Communication is from unknown users or that you have not requested. Do not reply in any case to these emails.
- Check the links before clicking even if they are from known contacts. Be wary of shortened links or use some service to expand them before visiting them.
- Be wary of attachments, even if they are from known contacts.
- Always update OS and antimalware from official repositories. In the case of antimalware, also check that it is active.
- Only install applications allowed and necessary for the work that comes from official sources.

- Cybercriminals take advantage of vulnerabilities or security holes in software, operating systems, or firmware.
- The more up to date the systems you use, the more difficult it will be for them to attack you.
- Turn on or Confirm auto-updates for Operating Systems & Software and set auto-updates to convenient time to avoid business disruptions.

If your device or software is **too old** it may not auto-update and leave you susceptible to technical, software, and security issues.

Turn On Automatic Updates



Turn On MFA

MULTI-FACTOR AUTHENTICATION (MFA) IS SECURITY MEASURE THAT REQUIRES TWO OR MORE PROOFS OF IDENTITY TO GRANT YOU ACCESS.

REQUIRES A COMBINATION OF SOMETHING THE USER **KNOWS** (PIN, SECRET QUESTION), **PHYSICALLY** POSSESSES (CARD, TOKEN), OR **INHERENTLY** POSSESSES (FINGERPRINT, RETINA).

THE MULTIPLE LAYERS MAKE IT HARDER FOR CRIMINALS TO ATTACK YOU AND YOUR FIRM.

Strong Passwords

STRONG PASSWORDS ARE:

- **USED** WITH MULTI-FACTOR AUTHENTICATION
- **UNIQUE** – NOT A FAMOUS PHRASE OR LYRIC, AND NOT RE-USED
- **LONGER** – PHRASES ARE GENERALLY LONGER THAN WORDS
- **COMPLEX** – NATURALLY OCCURRING IN A SENTENCE WITH UPPERCASE, SYMBOLS, AND PUNCTUATION
- **EASY TO REMEMBER** – SAVE YOU FROM BEING LOCKED OUT

Passwords vs Passphrases

PASSWORD

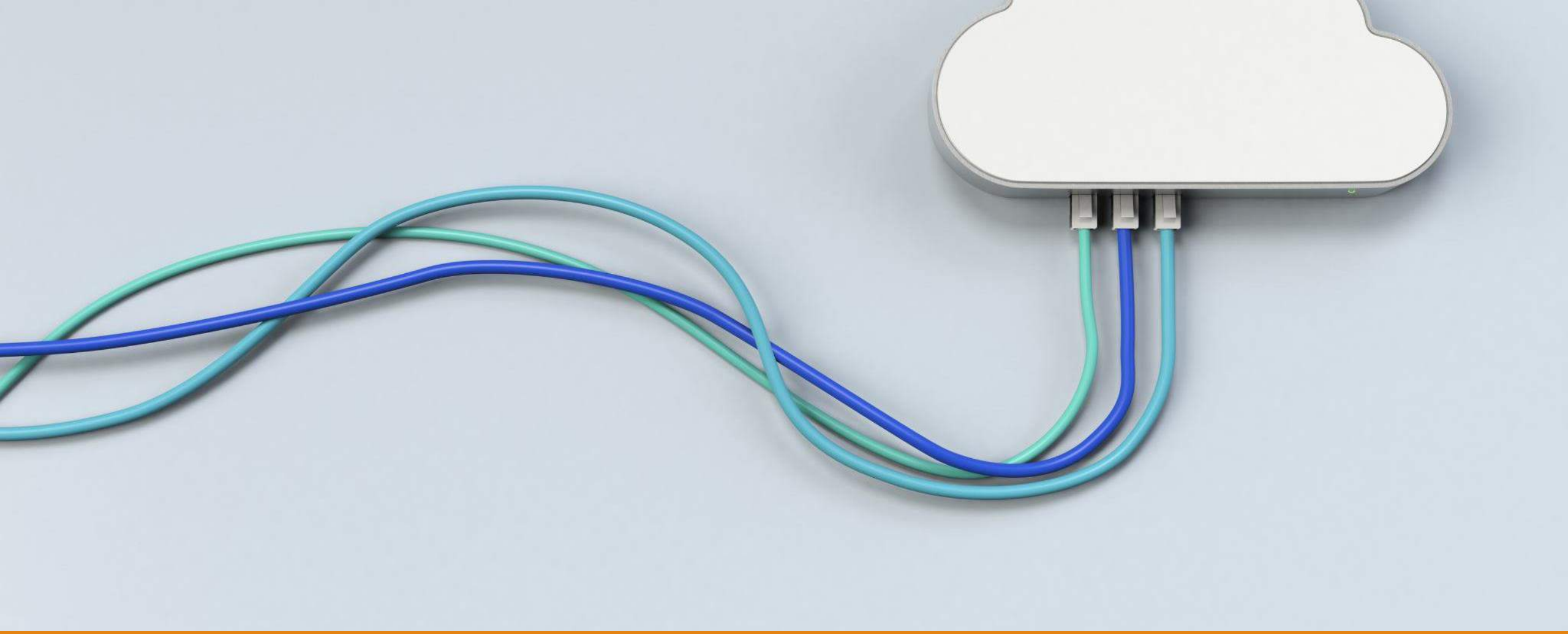
- A&d!8J+1
- Mildly complex
- Hard to remember
- Easy to crack on a targeted attack
  - Time to Crack - 150 minutes

PASSPHRASE

- I don’t like pineapple on my pizza!
- Mildly complex
- Easy to remember
- Hard to crack on a targeted attack
  - Time to Crack – 40 days
  - Excellent length, complex with apostrophe, exclamation mark and use of spaces

Access Control

- ACCESS CONTROL IS A WAY TO LIMIT ACCESS TO A SYSTEM. IT ALLOWS YOU TO:
  - Decide who would access to
  - How much access
  - For how long
  - Determine which roles require what access
  - Enforce staff access control limits
- HELP YOU PROTECT YOUR FIRM BY ALLOWING YOU TO LIMIT STAFF AND VENDOR ACCESS
- THE PRINCIPLE OF LEAST PRIVILEGE IS THE SAFEST APPROACH FOR MOST SMALL FIRMS
  - Users get the bare minimum permissions they need to perform their work.
  - Reduces the risk of an ‘insider’ accidentally or maliciously endangering your firm.



Backups

A DIGITAL COPY OF YOUR FIRM'S MOST IMPORTANT INFORMATION – CLIENT DETAILS & FILES.

Backups

- Make and keep at least **three** up-to-date backups on different media.
  - Keep at least three copies up to always date: specific hard drive for copies, external USB, and cloud.
  - Ideally store backups, whenever possible, on physical discs (DVD or Blu-Ray) or on external media not connected to your network).
  - If a “cloud backup” make sure is synchronized continuously.
  - Safely disconnecting and removing your back up storage device after each backup will ensure it is not impacted during a cyber incident.
- Check regularly that the backups you have stored are **working** properly and you know the **steps** to recover them.
  - Backups can also get corrupted.
  - Periodically check that backup copy, for which you must try to restore some files from time to time.

Encryption

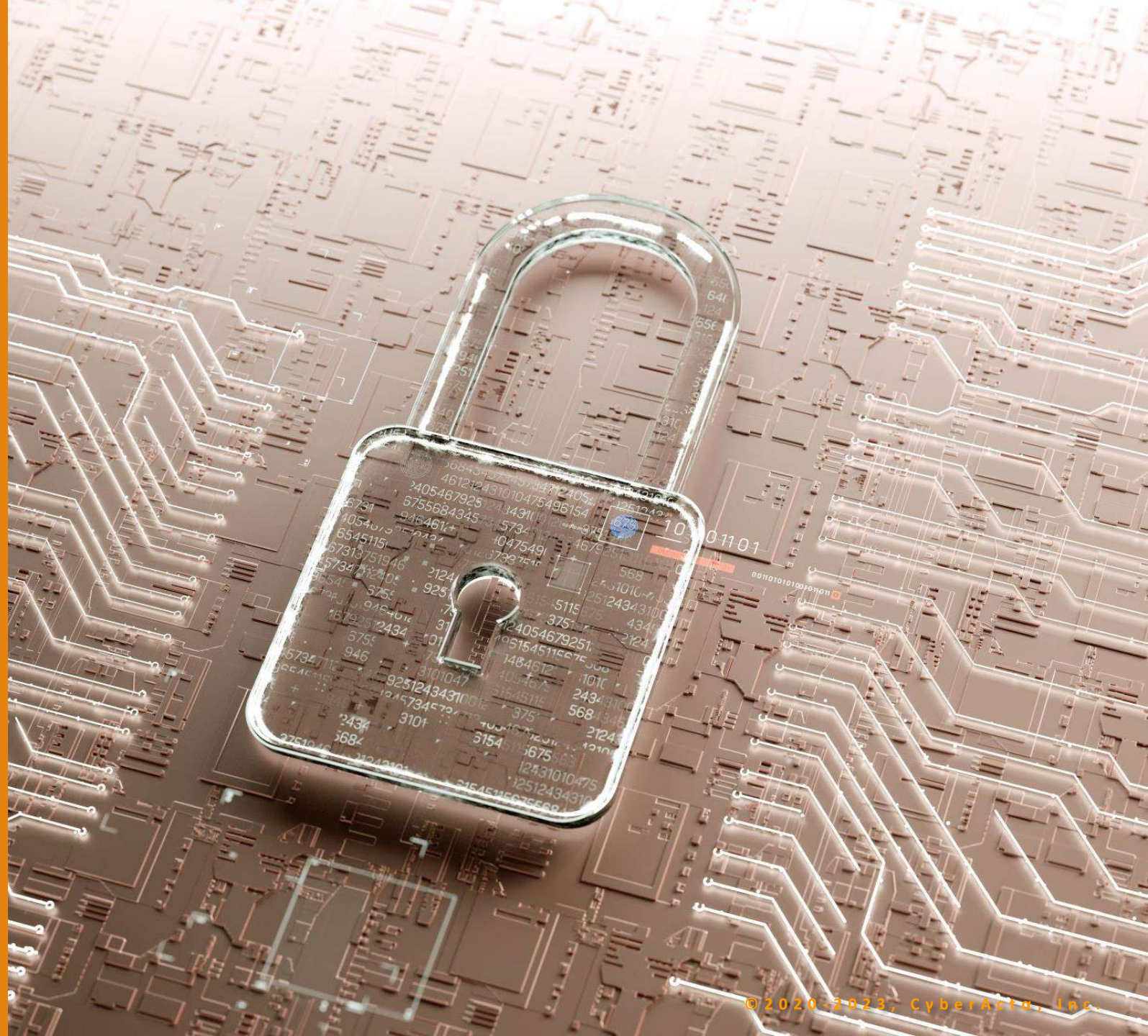
ENCRYPT THE MOST SENSITIVE INFORMATION SO THAT CYBERCRIMINALS CANNOT MAKE THE INFORMATION PUBLIC.

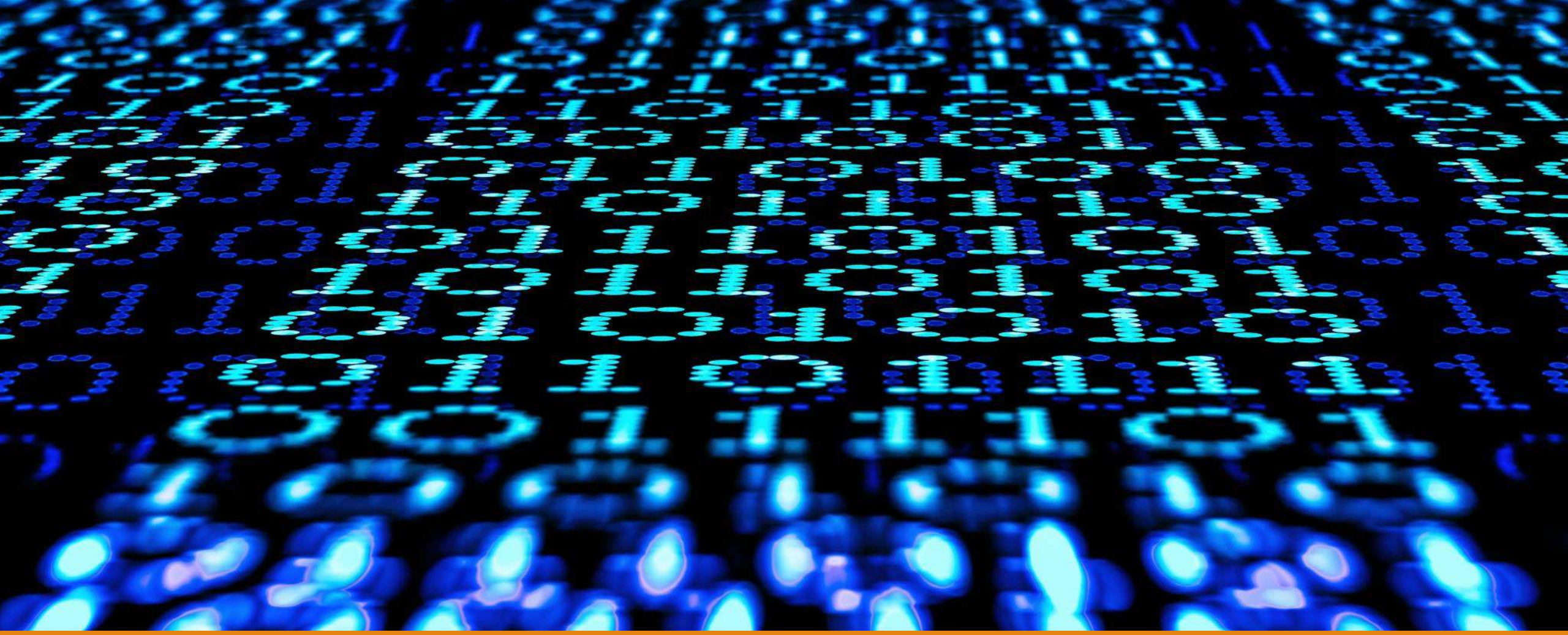
DO NOT SAVE THE ENCRYPTION KEY ON THE SAME DEVICE, AND IF YOU USE A CERTIFICATE TO DECRYPT IT, SAVE AND KEEP IT DISCONNECTED FROM YOUR COMPUTERS.

Microsoft Windows – BitLocker (FREE)

Apple – iOS FileVault (FREE)

IF ENHANCED CYBERSECURITY IS WARRANTED, THEN VISIT https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/





Long Term Investments

INCIDENT RESPONSE PLAN

Incident Response Plan

- A great preventive action to respond to incidents.
  - Carry out the management of incidents within the firm;
  - Documentation necessary on the systems and networks that are used in the firm.
- Define what is normal activity that would allow you to detect suspicious activities.
- Classify the incident so you establish nature, origin and potential impact – **FAST**.
- Escalate the incident, if you do not have resources to solve it, or you need to have external experts for its resolution.
- Once the incident is closed, we must record all the necessary data about it: affected users, equipment, what actions have been taken, results, etc. With this, improvements can be detected to act in case a similar incident is repeated.

Key Areas In Your IRP