10 Ways to Improve Your Cyber Security

October 29, 2021

Barry Mathis, PYA

A Few Statistics & Trends

2020 Statistics

- In 2020, the average business cost of a cyberattack is $3.86 million and it required over 200 days to detect the breach (IBM)
- 68% of business leaders felt the risk of a cyberattack increasing (Accenture)
- A majority of cyberattacks are motivated by financial gain, nearly 86%. The second leading motivator of a cyberattack includes state espionage. (Verizon)
- Ransomware attacks cost businesses an estimated $20 billion in 2020, having grown by over 50 times since 2015. (Cybersecurity Ventures)
- Malicious email attacks are up 600% in 2020, fueled by the pandemic. (ABC News)
- Statistics continue to show social engineering playing a part in a vast number of breaches. This includes malicious tactics such as phishing attempts, baiting, and tailgating

2022 Trends

- Working from home poses new cybersecurity risks and is one of the most talked-about new trends in cyber security.
- IoT (Internet of Things) - additional devices change the dynamics and size of what is sometimes called the cyber-attack surface – that is, the number of potential entry points for malicious actors.
- Cyber attacks on all businesses, but particularly small to medium sized businesses, are becoming more frequent, targeted, and complex.
- Phishing attacks are currently the most extensive security threat to the IT sector, with many still falling victim to phishing emails. Since cybercriminals use more advanced methods to create well-executed business email compromise attacks (BEC), phishing emails and malicious URLs remain prevalent on the web, except that they are now highly localized, more personalized, and are geo-targeted.

10 Securely Backup Data

PYA

Backup and Test Restore

- Backing up data securely and properly is required
- Often, testing the ability to restore any compromised or lost data is overlooked
- Current tactics being used by Bad Actors is to compromise the backup before enabling ransomware
- Restore should be tested and validated regularly
- Just because it is in the cloud, does not guarantee your ability to recover lost data

9 Strong Policies and Protocols

Policies, Procedures and Protocols

- The core step to implementing a successful information policy is ensuring that staff members understand the steps they are taking as well as the reasons for taking those steps. If the staff believe your information security policies are too restrictive or that they are being treated as if their time and effort are not valued, they will subvert the security system to ease their own workflow.
  - Keep policies simple, easy to understand and easy to reference
  - Seek advise on standards
  - Don’t let convenience dictate security standards
  - Audit often

8 Protect Mobile Devices

Encryption is Standard

- Where it is necessary to commit electronic health information to a mobile device, cybersecurity experts recommend that the data be encrypted.
- Mobile devices that cannot support encryption should not be used.
- Encrypted devices (and software) are readily obtainable at a modest cost — much less than the cost of mitigating a data breach.
- If it is necessary to take a laptop containing electronic health information out of a secure area, you should protect the information on the laptop's hard drive through encryption .
  - Encryption should be pre-boot full disk
  - Verified by security professional
  - Documented to include version, date and time

7 Practice Incident Response Plan

Have a plan

- A data breach response plan is a proactive way to be prepared in the event that a breach does occur. Having a risk management strategy in place to combat incidents such as breaches can minimize the impact on your company and bottom line. An incident response plan, for example, provides guidance for your team during the phases of detection, containment, investigation, remediation, and recovery

- Conduct tabletop exercises annually

6 Governance & Oversight

Make IT Security a Business Factor

- Security governance is the means by which *you* control and direct *your* organization's approach to security. When done well, security governance will effectively coordinate the security activities.
- It enables the flow of security information and decisions around your practice or hospital.
- Just as security is the responsibility of everyone within an organization, security decision making can happen at *all levels*. To achieve this, an organization's senior leadership should use security governance to set out the kinds of security risks they are prepared for staff to take, and those they are not.

5 Conduct Risk Analysis Annually

Start with an Assessment

- Required under federal standards
  - HIPAA
  - Incentive based payment programs
- Without a risk assessment to inform your cybersecurity choices, you could waste time, effort and resources – there is, after all, little point implementing measures to defend against events that are unlikely to occur or won't have much material impact on your organization.
- Likewise, it is possible that you will underestimate or overlook risks that could cause significant damage to your organization.

4 Secure protocols with vendors

Trust but Verify

- Third-party vendor management policy is perhaps the most underrated component to a mature cybersecurity strategy. Last year, *Becker's Hospital IT* reported :
  - *"Although data breaches are rare, almost half – **44 percent – are caused by third-party vendors**, according to an esentire survey.*
    - *Of the data breaches that happened from a vendor, only 15 percent of firms affected reported that the vendor informed them when a breach happened."*
- Within your vendor management policies and procedures, you should outline:
  - How you select your third-party vendors
  - When and how you perform vendor risk assessments
  - Necessary legal clauses to include in contracts with third-party vendors
  - Cybersecurity risk reporting measures
  - How your team will monitor vendor risk

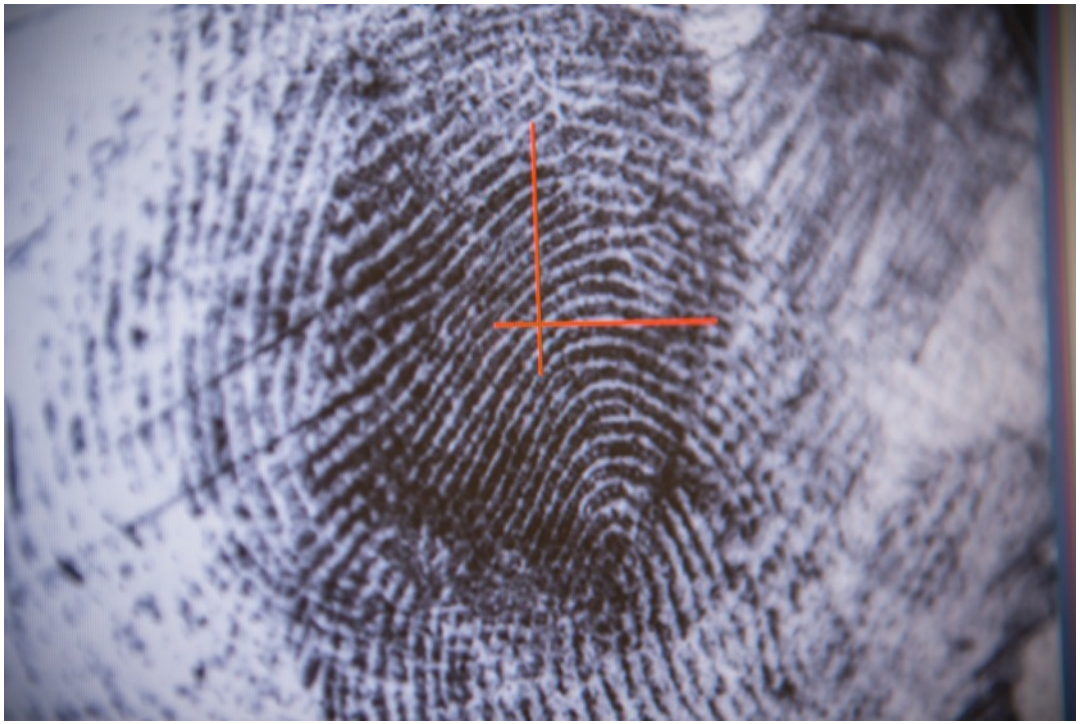
3 Keep Systems Up To Date

PYA

Software and Hardware Updates

- When patches are released to the public, the vulnerability often is disclosed with it. If you were an attacker, would you spend weeks or months trying to find a vulnerability, or read up on the latest patch for a third party component and bet on the fact that most users are not fast enough to apply them?
- If you take into consideration the fact that only 10% of the code base in an average application is written in house and that 21,000 known vulnerabilities (CVEs) were reported in the last 18 months, you'll understand that known vulnerabilities have become the weakest link in your software security.
- While you are patching operating systems for your servers and endpoint devices, don't forget that patches need to be applied to vendor products integrated into your environment, not to mention patching your own software is a key piece of the cyber security risk management.

2 – Multi Factor Authentication



Passwords are not enough

- Multi-factor authentication (MFA) means that to access software or carry out a transaction, at least one more means of personal verification is needed
- This could be as simple as entering a memorable word or using a passcode from a text message or dedicated App
- Microsoft: A study noted by Microsoft found that implementing MFA was successful at blocking 99.9% of fraudulent sign-in attempts. Google: A study noted by Google found MFA to be **between 76% to 100% effective** at blocking account hacks. There's a range because it depends upon the method used

1 – Education, Education, Education

Continuous Awareness Training

- Educate and train employees and stakeholders on best practices to prevent or reduce breaches that target insiders, such as phishing. Think of awareness and action across the enterprise as a human firewall
- Employees, and their access to protected data, are now the primary target of hackers
- Gaining access to an employee's login information allows them to impersonate staff, or their computer, to gain access to clinical and financial systems and data
- Technology can address only a fraction of security risks
- Awareness training is not a checkbox, or once a year activity
- Test and reward your employees

Resources

- Gartner Forecast Analysis on Information Security (Premium)
- Verizon 2020 Cybersecurity Report
- Symantec's Internet Security Threat Report
- 2020 Q3 Data Breach Report by Risk Based Security
- Cisco's Cybersecurity Reports
- Cost of Data Breach Report by IBM
- McAfee Labs Threat Reports

Questions:

Barry Mathis

Bmathis@pyapc.com

PYA, P.C.

800.270.9629 | www.pyapc.com