UHY Staffing Webinar Cybersecurity

Solutions for Data Privacy and Cybersecurity

Luke Nelson
Managing Director
Cybersecurity Solutions

Learning Objectives

- Understand what cyber techniques are being utilized by today's sophisticated actors
- Realize the changing ways in which cyber risks are impacting staffing organizations
- Learn how to protective and mitigating measures must be deployed holistically

Discussion for Today

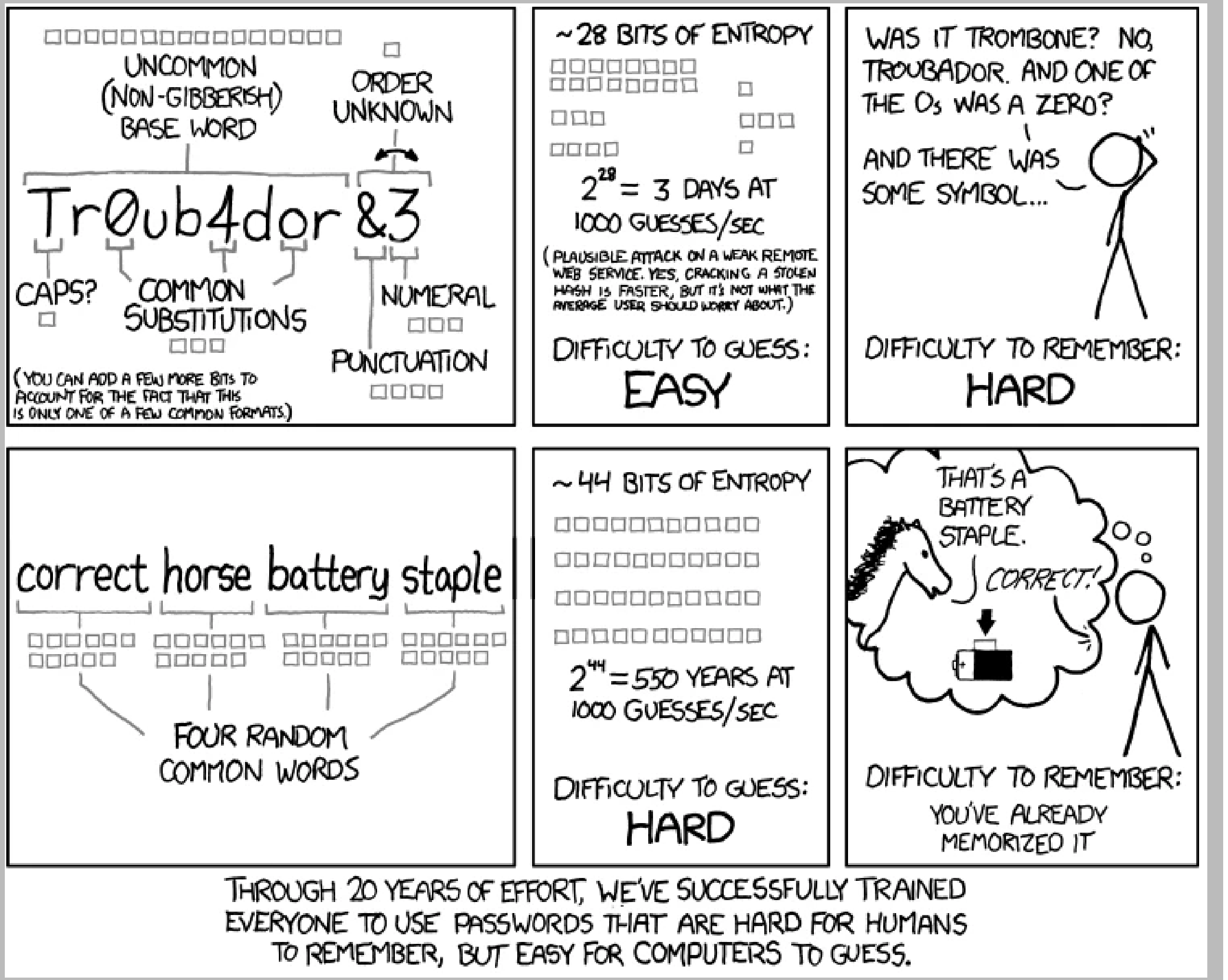
According to the 2022 Verizon Data Breach Investigations Report, approximately 78% of action vectors were through web applications or email during a breach. We are going to speak on three areas that we see for important for staffing organizations:

- User Credentials
- Ransomware
- Vendor Risk Management

User Credentials

User Credentials

- For almost everything we do in today’s world, we need credentials, typically a username and password. Password requirements typically suggest characteristics such as:
  - Complexity
  - Non-Repetitive
  - Frequency of Change
  - Multifactor Authentication (MFA)
- **“Security at the expense of usability comes at the expense of security.”**
  - If your “secure system” isn’t easy to use, people won’t use it, negating the security benefit.
  - We see this often with clients and maybe even ourselves. So, what is an alternative to this? A passphrase…


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

- Passwords vs Passphrase
  - A passphrase is a kind of password that uses a series of words, separated by spaces or not (it doesn't really matter).
  - "correcthorsebatterystaple" is the passphrase in the comic.
  - Although passphrases often contain more characters than passwords do, passphrases contain fewer "components" (four words instead of, say, 12 random characters).
  - This makes passphrases easier to remember, typically by using a mnemonic device.
- Passphrase Creation
  - Four words should be sufficient. Five words is better.
  - Don't choose from the most common words, and don't choose quotes or sayings.
  - Use a unique passphrase for every account you own.

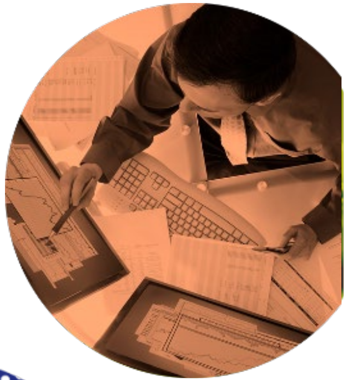
Real World Scenario

- Confidential Financial Forecast Spreadsheet
  - While discussing the current state of a staffing organization’s FP&A process we were informed that access to financial forecasts are kept in a corporate wide shared drive that is secured with a password.
  - Follow Up Questions:
    - Who is aware of the password?
    - How often is it changed?
    - Who changes it?
    - Where is the updated password stored?
  - It is not unusual for companies to store passwords in a separate location that is also shared externally.
- What can you do to protect and mitigate?
  - Information Security Policy and Procedure Review
  - IT Security Internal Controls Evaluation
  - Security Risk Management Methodology Assessment

Ransomware

Ransomware

- What is Ransomware?
  - Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
  - Malicious actors then demand ransom in exchange for decryption.
- How does a company protect itself?
  - Be Prepared. Have secured backups and response procedures for when a ransomware attack happens.
  - Ransomware Infection Vector. Know and understand how you could be infected with ransomware, such as phishing, web vulnerabilities, third party vendors, etc.



Key Ransomware Questions

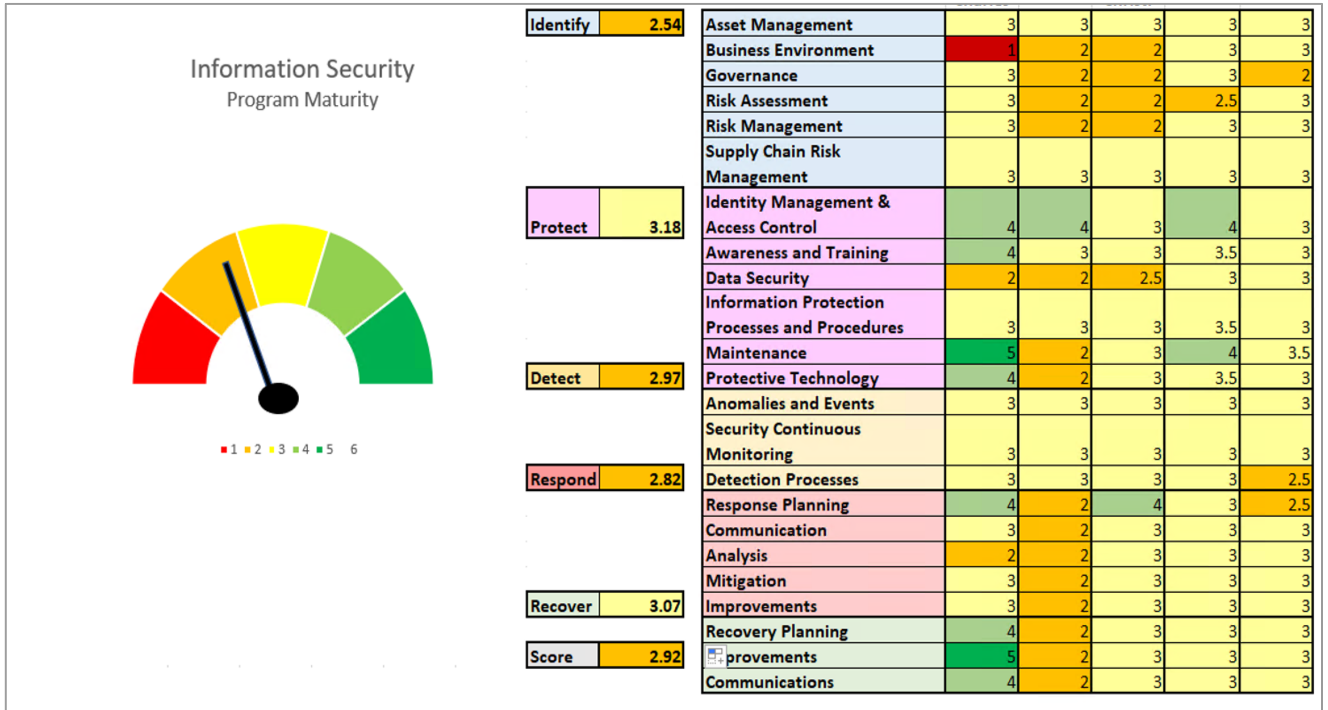
- **Backups**
  - Do we backup all critical information?
  - Are the backups stored offline?
  - Have we tested our ability to revert to backups during an incident?
- **Risk Analysis**
  - Have we conducted a cybersecurity risk analysis of the organization?
  - Do we prioritize action for areas of most risk?
- **Staff Training**
  - Have we trained the company on cybersecurity best practices?
  - How often does training occur?
- **Penetration Testing**
  - Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?
  - How often do we update our approach to penetration testing and social engineering?
- **Vulnerability Patching**
  - How are system vulnerabilities identified, tracked and monitored?
  - Have we implemented appropriate patching of known system vulnerabilities?
- **Business Continuity**
  - Are we able to sustain business operations without access to certain systems?
  - What is the impact to the company if key systems are unavailable?
  - Have we tested our Business Continuity plan?
- **Incident Response**
  - Do we have an incident response plan?
  - Have we tested and exercised it?
  - Do we have incident response support agreements in place?

Real World Scenario

- Accounts Payable
  - An Accounts Payable clerk was sent an email stating the staffing company was past due on an invoice. The email states to click on an attachment to view the outstanding statement.
  - The Accounts Payable analysts clicks on the attachment and releases malicious code gaining access to their AP system and locking out all users.

What can you do to protect and mitigate?

- Security Controls Assessment
- Rapid Incident Response Support
- Network Intrusion Protection Evaluation
- Security Awareness Training / Campaigns



Identify	2.54	Asset Management	3	3	3	3	3
		Business Environment	1	2	2	3	3
		Governance	3	2	2	3	2
		Risk Assessment	3	2	2	2.5	3
		Risk Management	3	2	2	3	3
		Supply Chain Risk Management	3	3	3	3	3
Protect	3.18	Identity Management & Access Control	4	4	3	4	3
		Awareness and Training	4	3	3	3.5	3
		Data Security	2	2	2.5	3	3
		Information Protection Processes and Procedures	3	3	3	3.5	3
		Maintenance	5	2	3	4	3.5
Detect	2.97	Protective Technology	4	2	3	3.5	3
		Anomalies and Events	3	3	3	3	3
		Security Continuous Monitoring	3	3	3	3	3
Respond	2.82	Detection Processes	3	3	3	3	2.5
		Response Planning	4	2	4	3	2.5
		Communication	3	2	3	3	3
		Analysis	2	2	3	3	3
		Mitigation	3	2	3	3	3
Recover	3.07	Improvements	3	2	3	3	3
		Recovery Planning	4	2	3	3	3
Score	2.92	provements	5	2	3	3	3
		Communications	4	2	3	3	3

Figure 1: Overall Scorecard

SaaS Vendor Risk Management

SaaS Vendor Risk Management

- Companies are becoming heavily reliant on Software as a Service (SaaS) to assist in their day-to-day operations.

- The ease of purchase of SaaS product can lead to a challenge in successfully managing the growing number of vendors and more importantly, the number of vendors with your data.

Key Vendor Risk Questions

- Are the necessary security considerations in place in the contract to reflect the company’s security requirements and/or customer’s requirements?
- Does the company know who all the SaaS vendors are that are being used throughout the organization (potential Shadow IT)?
- Does the company understand the controls that must be in place to ensure the SaaS application is implemented as designed (such as access controls of user accounts, etc.)?
- Does the third-party audit(s) the vendor undergo apply to the company use case?
- Does the company understand the vendors that the SaaS is using and the potential risks that apply (4th party risk)?
- Does the company understand what data is being provided to the SaaS, how long it is retained, can it be deleted, verification of data disposal, and can data be extracted if moving to a new application?

Real World Scenario

- Year End Close Activities
  - During year-end close activities, the staffing company's financial module within their SaaS based ERP system was kicked offline.
  - Contract Service Level Agreement (SLA) metrics state 99.7% uptime during normal course of business.
  - The company could not get in direct touch with vendor and resumption of services was unknown.
  - Prior to resumption of services the company was informed the root cause of the issue was due to a cybersecurity breach.
- What could you do to protect and mitigate?
  - Cyber Risk Exposure Analysis
  - Business Continuity and Disaster Recovery Planning
  - Vendor Risk Management Policy Review
  - Data Governance and Mapping

Questions

Luke Nelson
Managing Director
lnelson@uhy-us.com