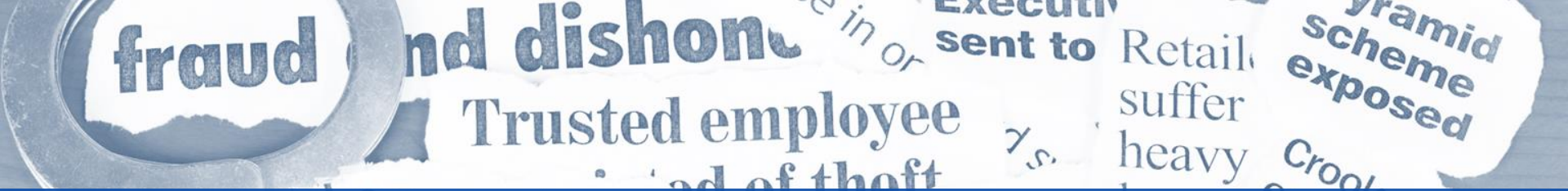
DANNIBLE & MCKEE, LLP

Certified Public Accountants and Consultants

Delivering **Confidence**



FRAUD, IT'S NO LONGER JUST INTERNAL

Presented by:
Sean Daughton, CPA, CFE
Robert Reeves, CPA, CFE

November 9, 2023

Agenda

- What is Cyber Fraud?
- Why is Cyber Fraud committed?
- Recent trends in Cyber Fraud.
- The Importance of Internal Controls.
- Common Types of Cyber Fraud That Exist in Businesses.
- Cyber Fraud Examples and Prevention Tips.

"Whoever commits a fraud is guilty not only of the particular injury to him, who he deceives, but of the diminution of that confidence which constitutes not only the ease but the existence of society."

- Samuel Johnson – Writer, Biographer, Editor

What is Cyber Fraud?

- Cyber fraud is any form of infraction, crime or fraud, carried out online using a digital platform, mobile application or network of computer systems.
- Cyber fraud can impact both individuals and organizations.

Types of Cyber Fraud

- Business email compromise;
- Identity theft and impersonation;
- Ransomware;
- Spoofing and phishing;
- Business and investment fraud;
- Piracy;
- Social engineering attacks; and
- Spam.

Technology Effect of Cyber Fraud

- Technology provides immediate and significant benefits to organizations, but it can also lead to significant exposure, exploited by fraudsters:
  - Rapid changes in technology can lead to unfamiliarity.
  - Users can be unaware of new technology advancements.
  - Perpetrators of cyber fraud take advantage of vulnerabilities of individuals and organizations.

Recent Trends in Cybercrime

- The pandemic caused a shift in job mobility and increased economic uncertainty, resulting in employees leaving or switching jobs more frequently.
  - **65%** of organizations reported data loss due to actions of insiders.
  - **44%** confessed to taking data with them.
- There has been an increase in the **transfer of data** between business and personal devices as a result of more employees working remotely, leaving businesses more **vulnerable** to cyber fraud.
- At a growth rate of **15%**, cyber fraud is up from $3 trillion in 2015 and is estimated to cost companies worldwide an estimated $10.5 trillion annually by 2025.
- In 2022, **70%** of businesses fell victim to **ransomware** attacks.
- As technology and AI advance, cyber fraud is becoming more **frequent**, more **targeted**, and more **sophisticated**.
- The NYS Comptroller released a report stating the main weaknesses in NY cybersecurity:
  - Use of unsupported applications;
  - Poor **access controls;** and
  - Lack of **monitoring** system changes.

Who's Behind Data Breaches?

Motives of Cyber Criminals

- **Financial Gain**: primary motive for most hackers; intention is to make a profit.

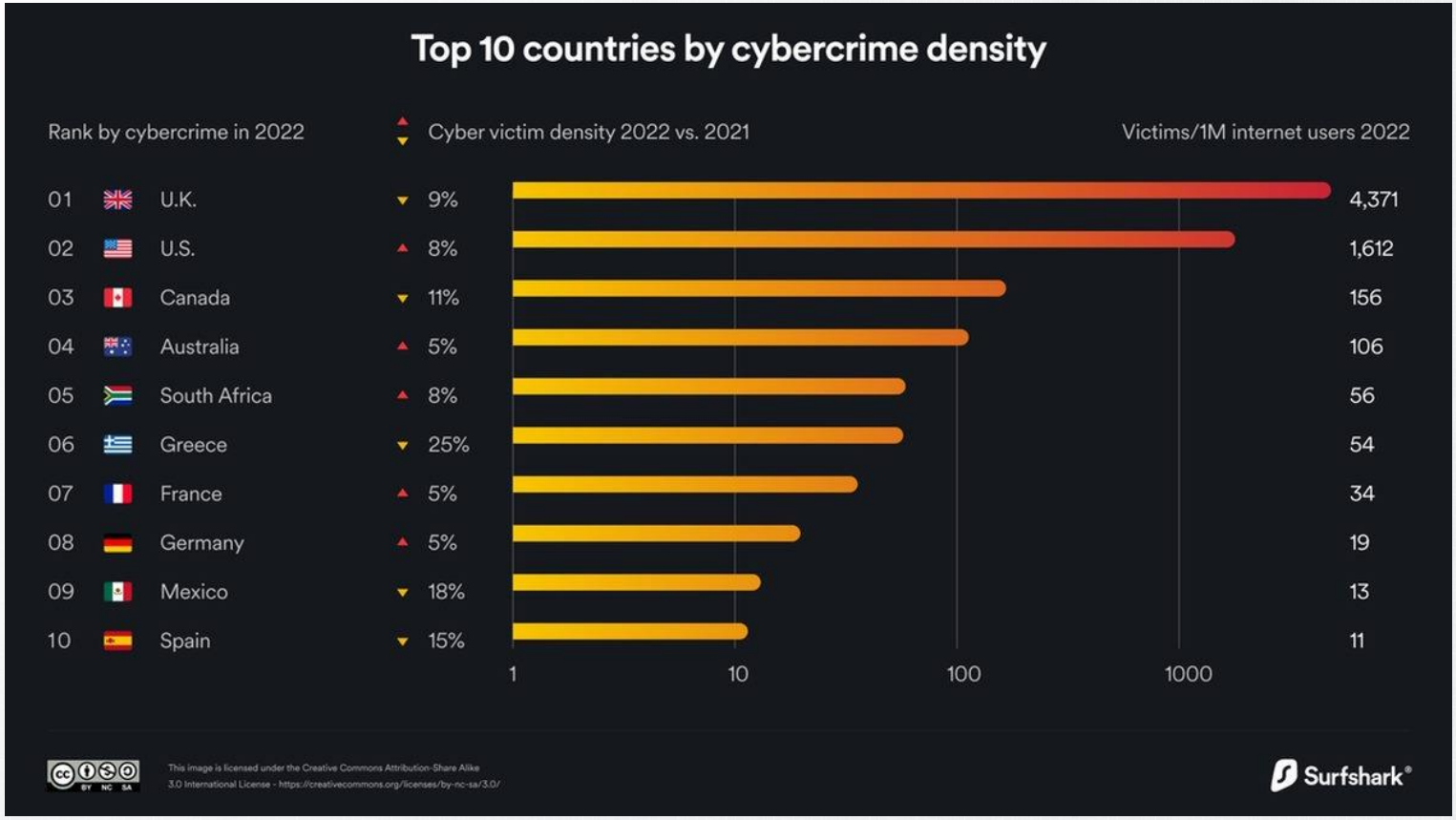
- **Recognition & Achievement**: hackers are looking for a feeling of achievement and want to be recognized for their feats.

- **Insider Threats**: 25% of cyber attacks; individuals provided with access take advantage of confidential information; unintentional causes include: carelessness, negligence, and compromised credentials.

- **Political Motivation**: these hackers are typically motivated by a particular cause or movement.

- **State Actors**: these hackers are acting on behalf of their own interest as well as the nation-sate that is providing them with financial aid and/or resources.

- **Corporate Espionage**: these hackers are looking to acquire a competitive advantage and usually steal statistical information.


Top 10 countries by cybercrime density
Rank by cybercrime in 2022
Cyber victim density 2022 vs. 2021
Victims/1M internet users 2022
01 U.K. 9% 4,371
02 U.S. 8% 1,612
03 Canada 11% 156
04 Australia 5% 106
05 South Africa 8% 56
06 Greece 25% 54
07 France 5% 34
08 Germany 5% 19
09 Mexico 18% 13
10 Spain 15% 11
1
10
100
1000
This image is licensed under the Creative Commons Attribution-Share Alike 3.0 International License - https://creativecommons.org/licenses/by-nc-sa/3.0/
Surfshark®

What Should Small Businesses Know?

- Cyber attacks on small and medium sized businesses are becoming more frequent and complex.
  - Approx. **43%** of attacks are aimed at small businesses because they have fewer controls in place.
- Types of Businesses most vulnerable to cyber attacks:
  - **Banks and Financial Institutions:** contain credit card info and bank account info.
  - **Healthcare Institutions:** contain health records, billing info, SS numbers, insurance claims.
  - **Corporations**: intellectual property, product concepts, marketing strategies, client and employee's databases.
  - **Higher Education:** enrollment data, financial records, personally identifiable info, and academic research.
- On average it takes a company **197** days **to discover** a data breach and up to **69** days **to contain** it.
- A slow response to a data breach can result in:
  - Loss of customer trust, productivity or major fines.

Back-to-back Incidents

- There are three common reasons many companies experience repeat data breaches:

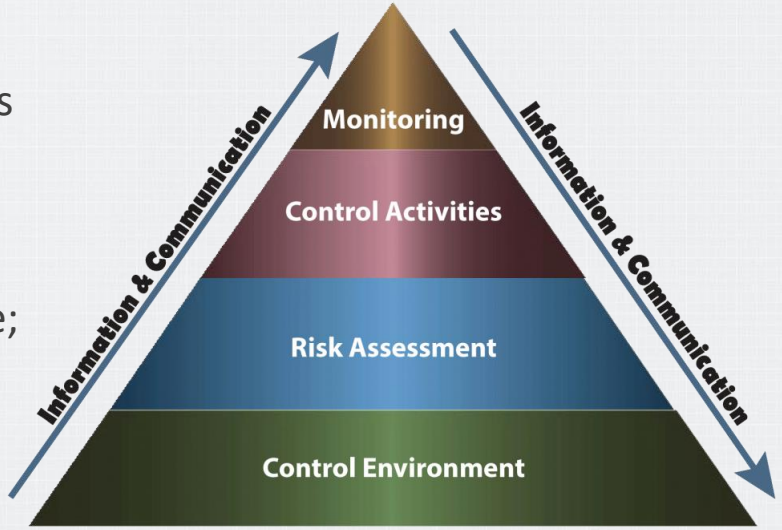
  1- Old vulnerabilities: Hackers will leave a secret window they can use to re-access a company's systems after a successful first attack;

  2- Human error: Employees using weak passwords leave a company vulnerable to multiple cyber attacks; and

  3- Malware: Hackers use malicious software to steal confidential information, so if a company fails to set up monitoring protocols after a data breach there is nothing stopping a repeat attack.

What Are Internal Controls?

- Internal controls are methods implemented by individuals within an organization to help with operations.
- There are 5 standards to internal control and each one is as important as the others to help companies function properly.
- The purpose of internal Controls:
  - To have assets remain protected;
  - To have records that are undoubtedly accurate;
  - To pertain operational efficiency;
  - To achieve objectives and goals developed by an organization; and
  - To guarantee that policies, rules, regulations and laws have been complied to by an organization.



The Five Internal Control Standards

- **Control Environment:** Establish structure, responsibilities, ethics, and reporting chain, ensure oversight is exercised by the board, and determine and plan goals for the organization.
- **Risk Assessment**: Analyze and identify potential risks, changes that impact internal controls, and practice Enterprise Risk Management ("ERM").
- **Control Activities:** Establish policies and procedures to mitigate risks, technology controls, departmental responsibilities, restrict access when necessary and maintain expenditure records.
- **Information and Communication**: Track information systems created for operations, goals, progress, and compliance, create separate lines of communication for confidential information and inform employees of these hotlines.
- **Monitoring**: Periodically evaluate internal controls, complete external audits, communicate control deficiencies and track corrective actions taken by management.

Information Security Controls

Information Security Controls play an important role in preventing internal and external threats of cyber fraud.

Examples:

- **Access Controls**
  - Physical and logical access restrictions.
- **Procedural Controls**
  - Cyber security awareness training, incident response plans and procedures and security framework compliance training.
- **Technical Controls**
  - Multifactor user authentication, antivirus software and firewalls, password strength requirements, encrypt network and/or computer files and VPN firewalls.
- **Compliance Controls**
  - Privacy laws and cybersecurity frameworks and standards and annual audits.

Growing Role of the CTO and CISO

- **Chief Technology Officer** is responsible for overseeing the development and distribution of technology to employees, external customers, vendors and other clients to improve growth of the business:
  - Software development;
  - Computer programming; and
  - “IT”.

- **Chief Information Officer** or **Chief Information Security Officer** is responsible for all IT infrastructure:
  - Cybersecurity;
  - Monitoring incident response activities;
  - Promoting cybersecurity awareness in the Company; and
  - Managing business disaster recovery.

Top Cybersecurity Threats for Businesses in 2023

Phishing

- Phishing is a scam where attackers deceive victims into revealing sensitive information.
- They disguise an email address, sender name, phone number or website URL by changing just one letter, symbol or number to convince you you're interacting with a trusted source to obtain:
  - Bank and credit card information; and
  - Passwords.

Common Phishing Email Features:

- Lucrative offers, prizes and discounts;
- Limited time offers and deals;
- Hyperlinks;
- Attachments; and
- Unusual sender.

Business Email Compromise (BEC)

- Business emails are top target of phishing hackers; and
- Leadership is most at risk as they have access to more valuable information.

Phishing

Phishing is still the most common form of cyber fraud. Technological advances have made phishing easier for hackers.

- Begins **91%** of cyberattacks.
- 2022 had the highest rate of mobile phishing in history.
- There has been a significant increase in other forms of phishing, including:
  - Vishing (voice phishing);
  - Smishing (SMS phishing); and
  - Quishing (QR code phishing).
- Hackers will use familiar names and brands to trick you into trusting the source.

Most Frequently Impersonated Brands	Approx. number of mentions
Microsoft (OneDrive, Office, etc.)	30,000,000
Amazon	6,500,000
DocuSign	3,500,000
Google	2,600,000
Adobe	2,000,000

Chat Generative Pre-trained Transformer (ChatGPT)

- Large language model-based chatbot developed by OpenAI and launched in November 2022.
- Enables users to refine and steer conversation towards a desired length, format, style, level of detail and language.
- By January 2023 it became the fastest growing consumer software application in history with 100 million users and a valuation of $29 billion.

How to use ChatGPT

1. Go to chat.openai.com or the mobile app, and log in or sign up (it's free).
2. Type your prompt in a message box on the home page.
3. Once ChatGPT spits out a response, you have a handful of options:
    1. Enter a new prompt;
    2. Regenerate the response;
    3. Copy the response; and
    4. Share the response.
4. Alternatively, if you know how to code, you can further use Python programming language to customize instructions in ChatGPT.

ChatGPT Uses

- Marketing:
  - Writing blogs
  - Targeted ads
- It has voice, video and image capabilities.
- Composing essays and emails.
- Optimize time by having ChatGPT brainstorm ideas, generate talking points, etc.
- Can even write code.
- Phishing uses (Vishing, Smishing, Quishing).

ChatGPT March 2023 Security Breach

- A bug in the open-source code used “beneath the hood” that allowed some users to see titles of other user’s conversations:
  - If you cancelled a request within a very specific timeframe, the system would get confused, and deliver your information to the next user who made a similar request because it didn’t know what to do with it.
- This breach was only a surface-level incident, after OpenAI dug deeper, they discovered this same vulnerability was likely responsible for visibility into users email addresses, payment, addresses, last four digits of SSN, credit card numbers and expiration dates.

OpenAI CEO Sam Altman

Chick-Fil-A Hacking

- Occurred in March 2023
- Data breach in the mobile app where personal information of 71,473 customers was exposed.
- The accounts were sold at a price range of $2 to $200.
- Through third-party accounts, the hacker was able to acquire email addresses and passwords.
- Examples of data acquired included:
  - membership numbers;
  - names; and
  - addresses.
- Chick-Fil-A began taking preventative measures to lower the chances of recurrence despite less than 2% of information being breached.

Indirect Proxy Method Phishing

- Occurred in June 2023
- Started with a phishing campaign against the employee of a company that acted as a trusted vendor to multiple organizations and bypassed multifactor authentication mechanisms.
- Attackers used a URL that pointed to Canva.com, a free online graphic design platform used for creating presentations, posters and other graphics.
- The URL linked to a page that mimicked a OneDrive document preview.
- Once clicked, the image took users to a fake Microsoft sign-in page to authenticate.
- After the email was compromised at the vendor, attackers extracted email addresses from existing email threads and sent out 16,000 more emails modified similarly to the malicious Canva URLs.
  - Attackers then monitored the victims' mailbox for undelivered and out-of-office emails.
  - Attackers also read emails from recipients who were suspicious of the authenticity of the phishing email and deleted from the user's mailbox.

Tips to Prevent Phishing Scams

- Avoid clicking links or opening attachments without carefully examining URLs.
- Don’t share personal information over text or email.
- Be weary of messages that are urgent and are requiring immediate action from you.
- Require regular **password changes** for accounts.
- Implement **conditional access policies** that evaluate sign-in requests using device identity signals like IP location or device status.
- Use **multifactor authentication** methods that cannot be intercepted, like **certificate-based authentication.**

DDoS attacks

- Distributed Denial of Service attacks (DDoS):
  - The attack focuses on manipulating the default or proper workings of network services, applications and equipment.
  - A company's internet is flooded with fake or illegitimate traffic (bots) to prevent true traffic from passing.
- Common types include:
  - Volumetric DDoS attacks (flood a machine or networks bandwidth with false data requests).
  - Application DDoS attacks (target weakness in an application).
  - Protocol DDoS attacks (targets the protocols used in transferring data to a crash system).
- Can result in:
  - hours of downtime;
  - immense costs; and
  - lost customers and reputation.

Microsoft DDoS attack

Occurred in June 2023

- The company identified surges in traffic against some services that temporarily impacted availability.
- Revealed that outages of its 365 services and Azure Cloud portal in early June were caused by a DDoS attack.
- A group called Anonymous Sudan claimed responsibility for the outages.
- In response, Microsoft has hardened their protection layers including tuning the Azure Web Application Firewall to better protect customers from similar attacks.

Tips to Prevent DDoS Attacks

- Know your businesses typical Internet traffic patterns.
- Put data centers on **different networks** (don't store all data in one place).
- Increase the bandwidth of your network so it can absorb a larger volume of traffic.
- **Regularly change passwords**
- These types of attacks are becoming more common and more severe, so take advantage of **anti-DDoS hardware** and software.

Ransomware

A form of malicious software, also known as malware:

- Crypto-ransomware – Encrypts hard-drives or files and folders.
- Locker-ransomware – Locks users out of their machines, without encryption.

Perpetrators of ransomware threaten users:

- Imply that users broke the law;
- Suggest they have possession of illegal/shameful acts done by victim;
- Time pressures for payment; and
- Indicate punishment for noncompliance.

Costs

- Data recovery costs;
- Forensic investigation;
- New control systems; and
- Lost time.

The FBI warns against paying the ransom as it does not guarantee you will get any data back.

Practice Resources, LLC

The Company was hit with a ransomware attack in April of 2022

- Practice Resources LLC provides billing services for dozens of hospitals and medical providers, like St. Joseph's, Crouse, Upstate Community Hospitals and Family Care Medial Group.
  - Family Care Medical Group (which is owned by the same doctors' group as Practice Resources) lost all its laboratory data and had to shut down for months while rebuilding their computer system.

  Examples of data acquired from over 942,000 patients:
  - Names, home addresses, dates of treatment and internal account numbers.
  - Billing records of several medical professionals.
- Patients weren't notified about the attack until August as it took several months to investigate which patients accounts info had been breached.
- Offered affected individuals a complimentary membership to an identity theft protection and credit monitoring service.

Yum! Brands

Occurred in January 2023 but wasn't announced until April 2023

- Parent Company of popular fast-food chains (KFC, Taco Bell, Pizza Hut).
- The Company originally thought only corporate data was breached when they were hit with the ransomware attack, but employee data was also compromised.
- Had to close multiple locations worldwide.
- Information obtained from hackers:
    - Worker's names, addresses, date of birth, social security numbers, and driver's licenses.
- The Company is now facing several class actions lawsuits from current and former employees alleging privacy violations.

Lawsuit: Christie Stinson vs. Yum! Brands

Damages to plaintiff's:

- Reasonably believe their PII is available for sale on the Dark Web as that is the motive of cyber criminals.
- Plaintiff has received spam calls, texts and emails multiple times a day, even after getting a new phone number.
- Costs of consulting legal counsel, credit freezes, purchasing credit monitoring services and running credit reports to check to suspicious activity.

Argument:

- Yum! has an obligation to keep personally identifiable information ("PII)" private and confidential.
- Vitim's weren't notified until three months after the data breach, could've lessened the damages if they were informed sooner.
- Arguing negligence on Yum! Brands and that the breach was a foreseeable risk that could've been prevented by:
  - Encrypting the network, computer files or the use of a firewall.

Tips to Prevent Ransomware Attacks

- Regularly **update** operating systems, software and applications.
- Use **strong passwords**.
- **Employee training** on security awareness.
- **Routinely back up** all system data on a separate system or network and consider **encrypting** it.
- Implement the use of **VPNs** and **firewalls** into security precautions.
- Avoid clicking links from unsolicited messages/emails.
- Create a **continuity plan** and/or **insurance** in case your business falls victim to this type of attack.

Identity Theft

- Misappropriation of personal, identifiable information:
  - Name, Birth date, SSN, medical records, employment and education.
- Perpetrator use of information:
  - Open lines of credit;
  - Purchase goods or services;
  - Obtain employment or prescriptions;
  - Purchase or rent property; and
  - Commit felonies and infractions.
- CPAs and financial professionals maintain records of client personal identifiable identity.
  - Obligation to protect information through controls and safeguards.

Powell Lacrosse

Occurred in January 2023

- The Company received 22,000 transactions for mostly the same item totaling $12.71.
- Several people who had never played lacrosse before called and asked for refunds.
- Hackers stole loads of credit card info, created a bot and used it to make multiple simple purchases in attempt to test and see if the credit cards worked.
  - This is a common tactic to test stolen credit cards with several small transactions.
- The purchases were flagged for fraud and the store had to disable credit card purchases.
- It was found that most of the people affected had the same bank and had not been previous customers of the store.

MGM Resorts

Occurred in September 2023

- Scattered Spider (also known as UNC3944) have claimed responsibility for the attack and said they've been in MGM Resorts' systems since 9/8/23. They're believed to be a subgroup of the larger ALPHV ransomware group. The hackers have told vx-underground that they used social engineering as an initial entry point.
- The hackers have told vx-underground that they used social engineering as an initial entry point. They were able to find an MGM Resorts employee on LinkedIn, impersonate them and call the organization's service desk to ask for access to their account.
- MGM implemented conditional restrictions that barred all access to their Okta (MGMResorts.okta.com) environment due to inadequate administrative capabilities and weak incident response playbooks. Their network has been infiltrated since Friday. Due to their network engineers' lack of understanding of how the network functions, network access was problematic on Saturday. They then made the decision to "take offline" seemingly important components of their infrastructure on Sunday.

MGM Resorts

Occurred in September 2023

- MGM Resorts said hotel and casino operations were back to normal, after more than 10 days of disruption to the company's casino, reservations system, digital room keys, payments and other operational issues.
- MGM Resorts has confirmed hackers stole an unspecified amount of customers' personal information during a September cyberattack.
- In a filing with the Securities and Exchange Commission, MGM Resorts reported that a recent cyberattack is expected to cost the company an estimated $100 million. Entertainment Group MGM Expects Insurance to Cover $110 Million in Cybersecurity Incident Costs.
- It seems that MGM wasn't the only casino chain hit by a recent cyberattack. Caesars Entertainment paid millions of dollars to hackers who breached its systems around the same time as MGM and was able to continue operations as normal. Caesars admitted to the breach in a filing with the Securities and Exchange Commission on September 14, where it said an "outsourced IT support vendor" was the victim of a "social engineering attack" that resulted in sensitive data about members of its customer loyalty program being stolen.

Case #1

- Receptionist at a healthcare organization noticed strange activity occurring on their computer and reported it.
- Further investigation discovered the Company's system had been breached.
- Company followed protocol and reported breach to proper Federal and State agencies as well as potential patients.
- Paid investigators, but no none could come up with an answer as to how their system was breached or any definitive answers on how much data was stolen.
- They had to assume all data on their computer system was breached.
- This delayed billings by a 2-4 weeks during this time frame.
- There was a ransomware policy in their insurance coverage, and they paid a $5,000 deductible:
  - Investigation costs;
  - Legal costs; and
  - Fines from HIPAA for violations of patient information (HIPAA still has not calculated this amount).

Case #2

- An employee clicked on an email link.
- A cybercriminal got into the Company's system and shut it down and held it for ransom.
- The company paid the ransom and got their system back up and running within 24 hours of the "blackout".
- The cybersecurity insurance policy covered the ransom amount.
- This incident put them behind about 3-4 months just from being down for 1 day.

Case #3

- Company holds proprietary information for customers (patented blueprints, formulas, etc.).
- Employee fell for a phishing email and the perpetrator was able to compromise the employee's computer and steal customer blueprints.
- The person contacted the Company and held the blueprints for a $1M ransom.
- Company paid the $1M to get their customer's property back.

Key Things to remember

- Training your employees about computer security.
- Have we purchased outside services to “target” our employees for training purposes? We use “Bullfish” internally that will send random emails out to our employees to determine if they have been trained enough or if they would open a file and put the Firm in jeopardy. (Cost is approximately $4,000 per year).
- Set up really good internal controls. Do a brainstorming session with your entire office staff. Ask the questions of what could happen. How do we handle an email from a superior about doing a wire transfer? Do we have procedures in place to go “outside” of the Company’s electronic environment? Remember, email servers have been a significant way data breaches have happened. Have we set up positive pay, are we constantly challenging our procedures? Have we had our CPA firm look at our controls to determine if things could be improved?
- Do we require a mandatory password change every 30 – 90 days?
- Have we considered setting up 2 factor verification for logins to our servers and emails?
- Review during your annual insurance renewal what types of coverage you have for employee dishonesty. What insurance do you have for a data breach. Does your insurance cover the cost of legal and forensic work?
- If you have a data breach is there a plan? The Company should have a team in place that focuses on what happens. If a data breach were to occur who do employees call? What are the next steps that the Company would immediately implement?

Questions

Sean T. Daughton, CPA, CFE
Audit Partner
sdaughton@dmcpas.com

Robert C. Reeves, CPA, CFE
Senior Audit Manager
rreeves@dmcpas.com