

The background is a teal color with a pattern of black lines and circles, resembling a circuit board or a network diagram. The lines are of varying thickness and connect various circular nodes, some of which are solid black and others are white with black outlines. The overall effect is a technical, digital aesthetic.

# "Cybersecurity in the Insurance Industry: Mitigating Risks, Protecting Clients, and Addressing the Dark Side"

---

Katrina Terry



## LIONFISH CYBER SECURITY

- Disabled vet-owned business focused on increasing cyber security protection and strengthening the digital security posture for small to mid-size companies.
- We want to help all companies across the US become Cyber Resilient.



## Katrina Terry, CEH

- Background in: Cyber Security Consulting / Digital Forensics / CEH / Bounty Hunting & Private Investigation
- Founder & CEO of LION195 Against Trafficking
- Business Champion at J.Galt Finance Suite
- US Navy Veteran – Operation Enduring Freedom





# The Impact of Cybersecurity Incidents

- **60% of small businesses** go under within six months after a ransomware attack.
- Cybersecurity Ventures predicts **cybercrime will cost the world in excess of \$7 trillion** annually by 2022, up from \$3 trillion in 2015. For organizations, the costs associated with cybercrime are vast.
- Recent studies have shown that the average cost of a data breach to Small Business can range **from \$120,000 to \$1.23 million**. And that's strictly limited to a small business market.
- With over **633,000 and counting cyber security Jobs unfulfilled** the chances of having enough trained cyber experts in typical consulting companies to help every business is unlikely.
- **Not enough trained cyber experts to protect the 33,000,000 business** across the country, we must be creative and bring proven methods to the fight.
- **CMMC Launched** and **Cyberspace Solarium Commission Report** released to address the national threat.

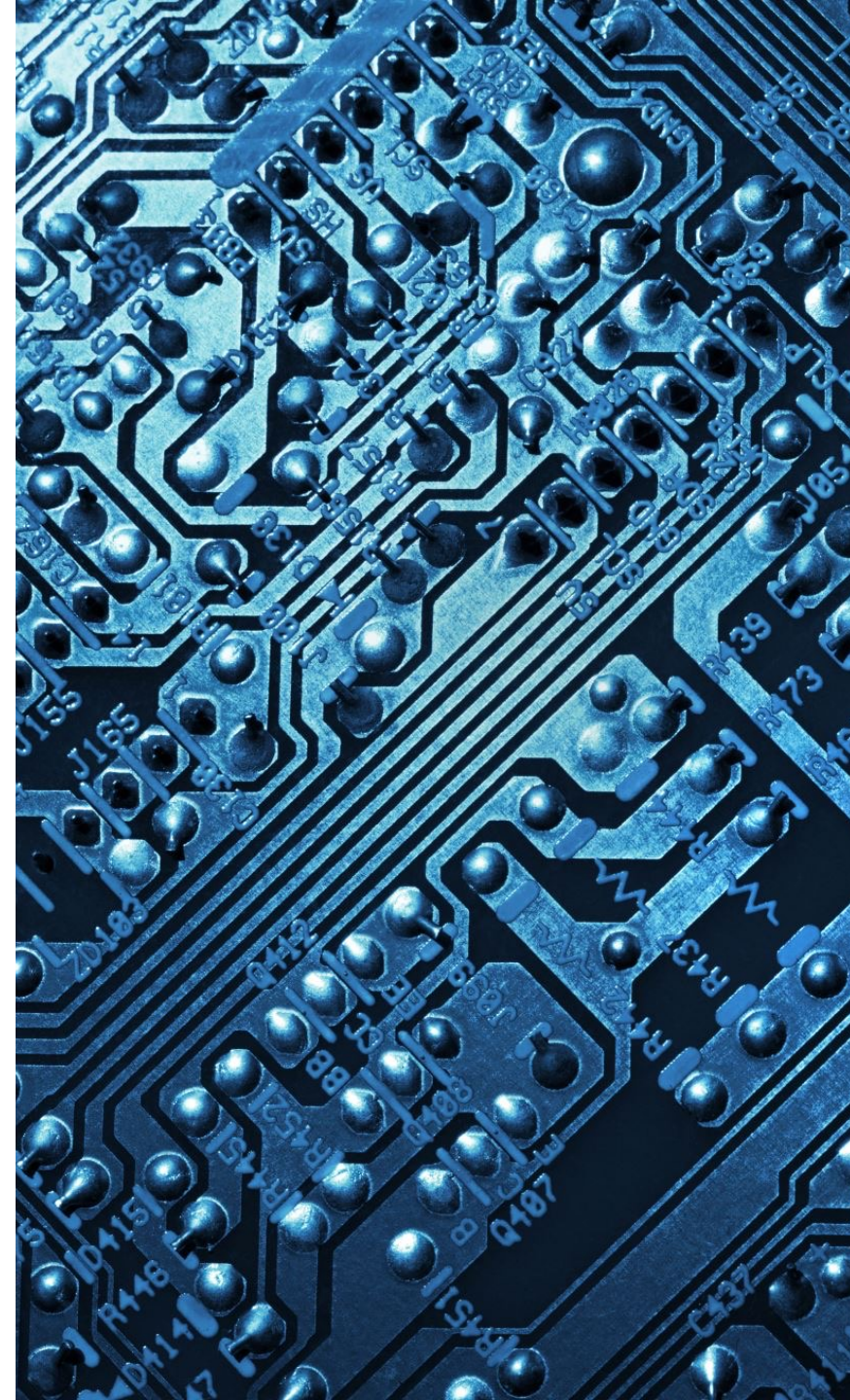


In short – SMB's are out matched with little resources to keep them protected at the level needed to compete in today's economy. By offering a battle tested approach along with cutting-edge technology and services at a reasonable cost, Lionfish can enable SMB's to survive with a Cyber Resiliency defense plan.



# Understanding Cybercriminal Tactics

- Exploring common attack vectors used by cybercriminals: phishing, ransomware, insider threats
- Analyzing motivations behind cyberattacks on the insurance and financial industry
- Discussing financial losses, reputational damage, and customer data implications
- Emphasizing the importance of proactive measures to prevent incidents





- This was previously an email example we would go by. However, hackers have significantly improved their skills in crafting phishing emails, making it increasingly challenging to detect such fraudulent attempts.







## PHISHING PREVENTION BEST PRACTICES

### **WATCH FOR OVERLY GENERIC CONTENT**

Cybercriminals send a large batch of emails. Look for examples like "Dear valued customer."

### **EXAMINE THE "FROM:" EMAIL ADDRESS**

The first part of the email address may look legitimate, but the last part might be off by a letter or may include a number in the usual domain.

### **LOOK FOR URGENCY**

"You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

### **CHECK ALL LINKS**

Hover over the link and see whether the link's description matches with the one implied in the email.

### **LOOK FOR ERRORS**

Notice misspellings, incorrect grammar and odd phrasing. This might be a deliberate attempt to try to bypass spam filters.

### **CHECK FOR SECURE WEBSITES**

Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

### **DON'T CLICK ON ATTACHMENTS**

Attachments containing viruses might have an intriguing message encouraging you to open them such as "Here is the schedule I promised."

## 3 STEPS TO PROTECT YOUR BUSINESS

### **CONDUCT REGULAR SECURITY AWARENESS TRAINING**

Keep your employees prepared to deal with any security threats that come your way by keeping them up to date on the latest security landscape and best practices through regular training.

# 1

### **PERFORM ROUTINE TESTING TO SEE WHETHER THE TRAINING IS EFFECTIVE**

It's critical to consistently evaluate the success of your security training through quizzes, surveys and mock tests.

# 2

### **DEPLOY QUARANTINING SOLUTIONS THAT STOP PHISHING ATTACKS**

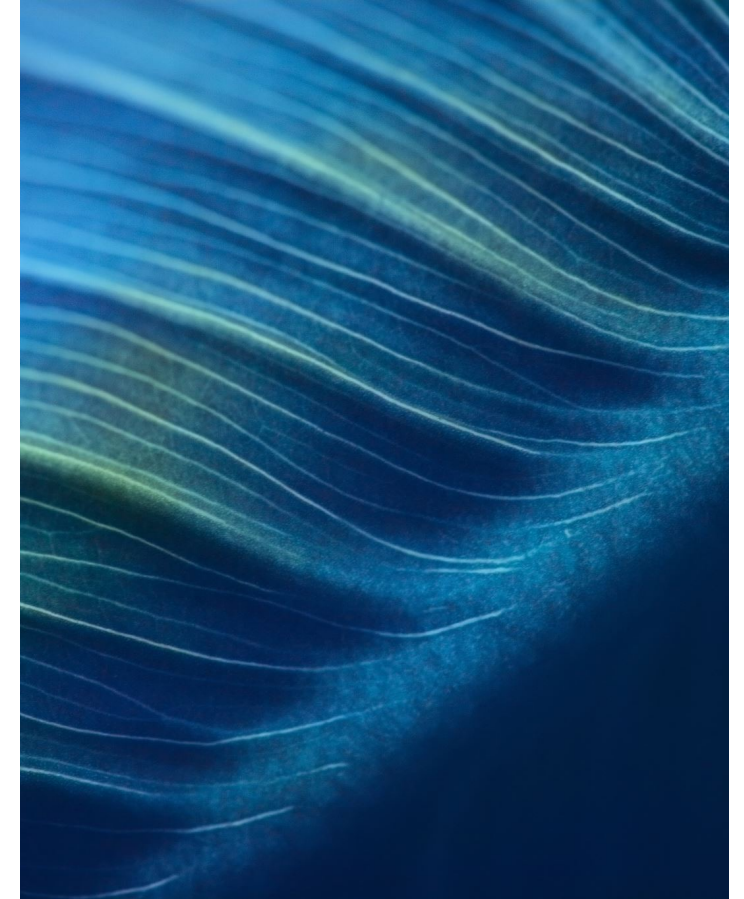
Businesses can protect themselves from the harmful effects of phishing attacks by deploying quarantining solutions that help stop phishing attempts in their tracks.

# 3



# Strengthening Cybersecurity Defenses

Implementing	Securing	Protecting	Building
Implementing a layered defense strategy (network segmentation, access controls, software updates)	Securing endpoints and mobile devices (endpoint protection, mobile device security)	Protecting sensitive client data (encryption, access controls)	Building a resilient incident response capability (incident response team, drills, external expertise)





# Employee Education and Awareness



Importance of cybersecurity awareness among employees



Examples of employee negligence leading to security breaches



Tips for creating a culture of cybersecurity awareness



# Third-Party Risk Management

- Risks associated with third-party vendors and partners
- Due diligence on vendors' cybersecurity practices
- Strategies for establishing and monitoring third-party security requirements






# 9 WAYS YOUR EMPLOYEES' WORK CREDENTIALS CAN LEAD TO A BREACH

When your employees use their work email on websites like the ones listed below, it makes your business vulnerable to a breach. With our Dark Web Monitoring, we can detect if your company is at risk due to exposed credentials on 3rd party websites.



## UNDERSTAND & MITIGATE YOUR RISK

 <b>EXTERNAL THREAT INTELLIGENCE</b> Are you monitoring for compromised data that can be used to exploit your business? YES <input type="checkbox"/> NO <input type="checkbox"/>	 <b>DATA BREACH &amp; PRIVACY LAW COMPLIANCE</b> Do you have a compliant data breach response plan in place? YES <input type="checkbox"/> NO <input type="checkbox"/>	 <b># OF EXPOSED CREDENTIALS FOR YOUR COMPANY</b> <input type="text"/>
--	---	---



# ACKNOWLEDGING THE DARK WEB

## (SURFACE) WEB

**The level where data is PUBLIC**

Only 4% of the web consists of indexed public websites that are visible to all web users through ordinary search engines such as Google and Bing.

## DEEP WEB

**The level where data is PRIVATE**

The largest part of the internet is made of protected information and is only located and accessed by a direct URL or IP address, that may require a password or other security access to get past public pages. That includes: email, online banking, social media pages & profiles, services such as video on demand, etc. It's used for legit purposes. Most of us access the Deep Web every day.

## DARK WEB

**The level where data is ANONYMOUS**

Within the Deep Web is the part of the internet called the Dark Web. A complex encrypted system not visible to traditional search engines that can only be accessed by a special browser called Tor. Transactions, IPs, profiles, locations, etc. are totally anonymous, making it the perfect place for many illegal activities to happen. It's not illegal by itself but that's where criminal sites live.

IS IT ALL BAD? NO. BUT IT'S QUITE BAD.



### WHAT YOUR DATA IS WORTH\*

TV On Demand Credentials.....	\$10
Scamming & Phishing Kits.....	Starting at \$100
Bank Account Credentials.....	Starting at \$200
Credit Card Information.....	Bulk sales available
Access to Corporate Network.....	\$120,000

\*Average prices based on recent Dark Web studies.

**61%**  
OF DATA BREACHES  
INVOLVED CREDENTIAL  
DATA

## IT WON'T HAPPEN TO YOUR BUSINESS. UNTIL IT HAPPENS.

Whether by user negligence or as a result of hacking, the chances of data exposure are high.  
The good news is that there are effective and affordable ways to prevent it.  
See some examples below.

#### CYBERSECURITY SOLUTIONS

Protect your business against internal and external threats with a comprehensive cybersecurity solution.

#### DARK WEB MONITORING

Get constant monitoring to ensure your company's data doesn't find its way to the Dark Web without you knowing.

#### SECURITY AWARENESS TRAINING

Teach your team how to ensure the links they click and websites they visit are authentic and not putting your business at risk.

CONTACT US TODAY TO FIND THE RIGHT SOLUTION  
FOR YOUR COMPANY

**STAY CYBER SAFE!**



# Case Studies and Dual Nature of Cybersecurity

## Sharing

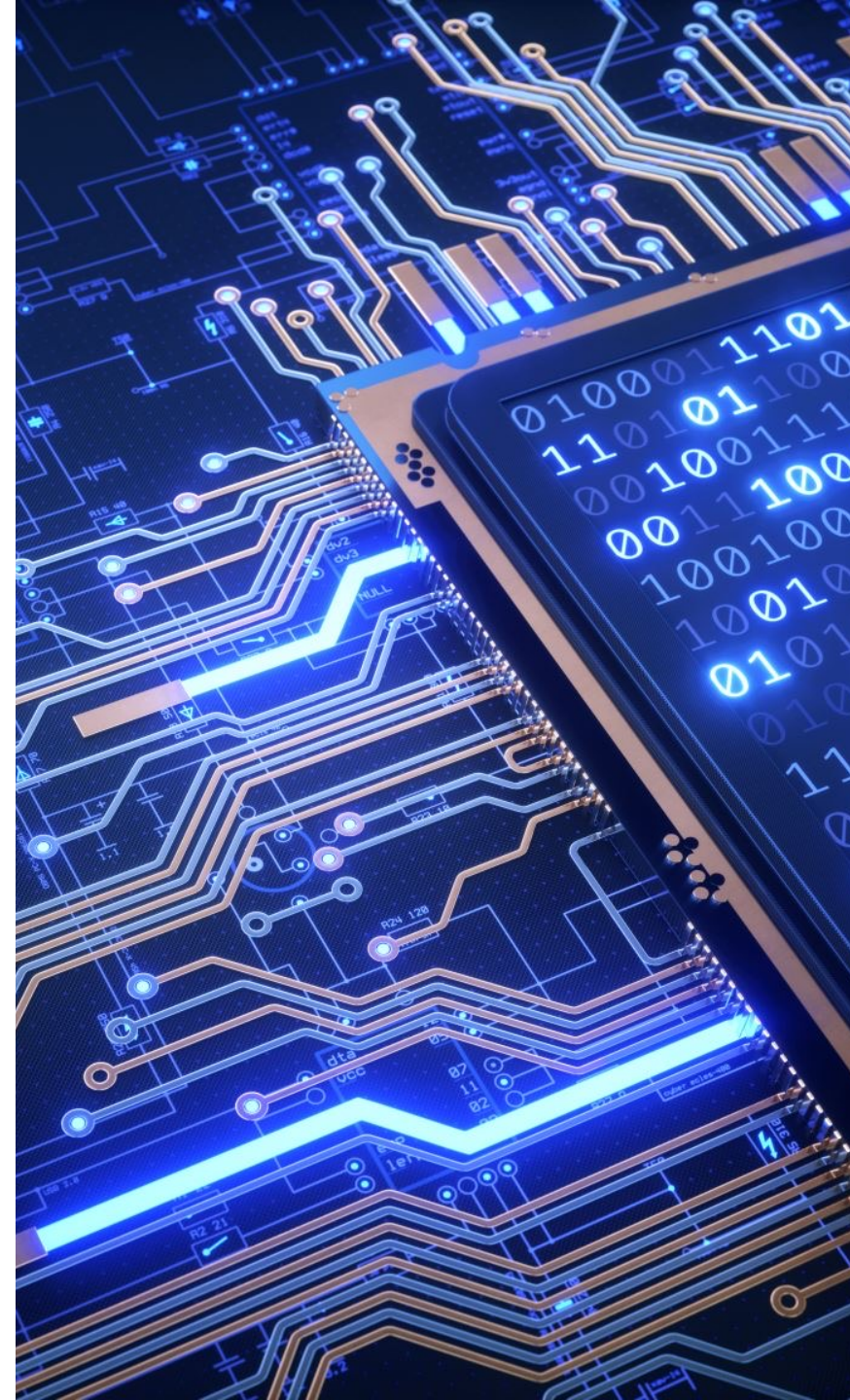
Sharing real-life case studies of cyberattacks

## Exploring

Exploring how cybersecurity aids in finding human trafficking victims and its dual role in this crime

## Tips for Implementing Online Safety

- Creating strong and unique passwords
- Enabling multi-factor authentication
- Being cautious of phishing emails and suspicious links
- Regularly updating software and applications
- Securing home networks and Wi-Fi connections
- Using secure file storage and backup solutions
- Being mindful of public Wi-Fi and shared devices
- Educating family members and employees on online safety practices







Thank you for your time! Feel free to reach out to me for Cyber Security Solutions & to learn more about LION195 Against Trafficking below.

Best contact info:

- Katrina Terry
- M: 317-459-9099
- [Katrina@LION195.ORG](mailto:Katrina@LION195.ORG)