DRAGNET

The importance of an Incident Response Plan

“I have an IR Policy”
An incident response policy(a broad, high-level framework for how an organization handles security incidents)

An incident response plan offers detailed, step-by-step procedures for responding to specific incidents. The policy defines the overall strategy, while the plan outlines the actions to be taken.

Think about the fear behind this….

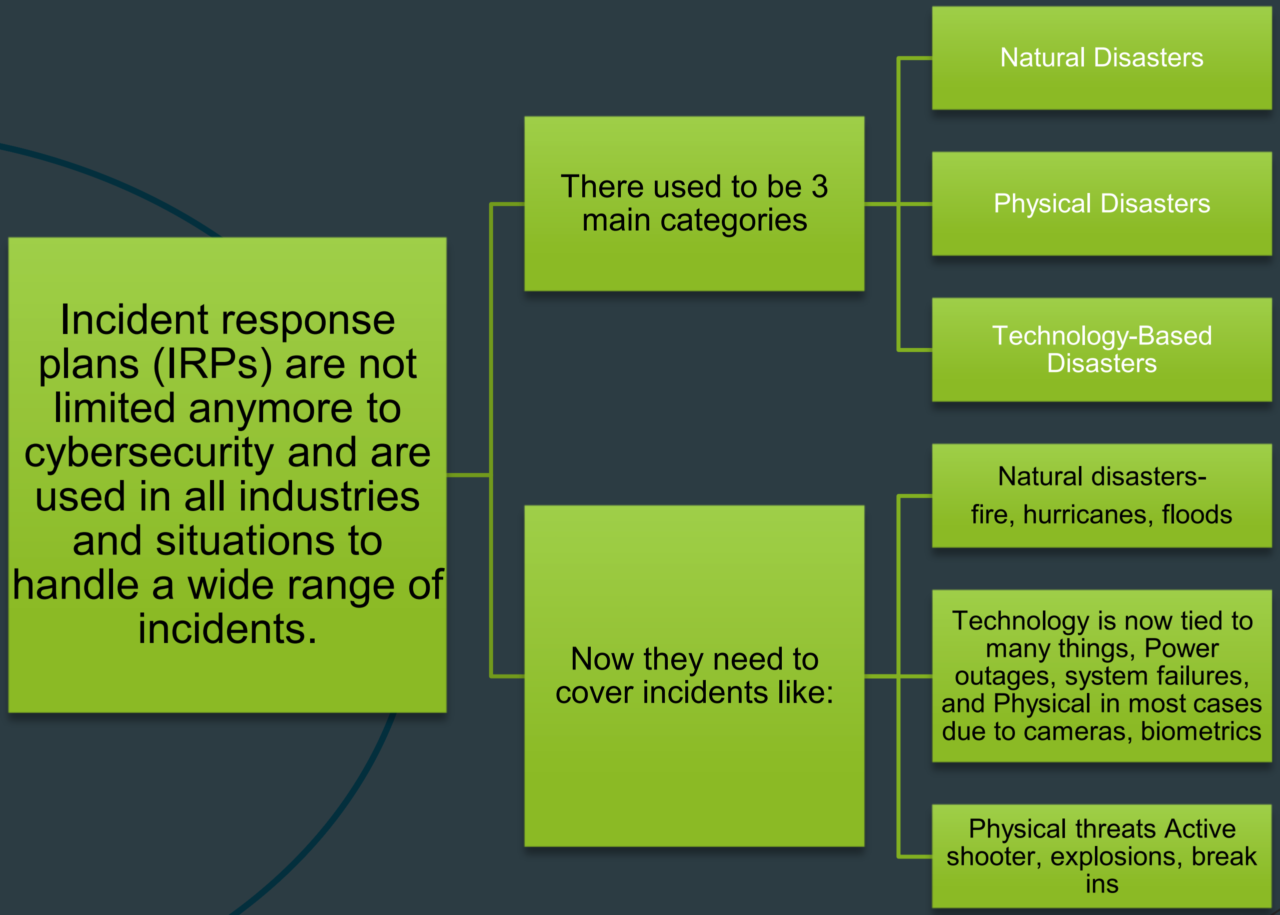
As many as 75 percent of companies have no IRP in place.

And that's a problem. Without an IRP, it's hard to minimize the damage of a security breach if you're unclear on what to do.

Why do I care about my incident response plan???

Failing to follow an incident response plan at work can lead to many legal issues for the organization, potential financial penalties, fines, lawsuits, and investigations from regulatory bodies.

Adhering to an incident response plan is crucial for the safety of employees, the protection of the company's assets.



Incident response plans (IRPs) are not limited anymore to cybersecurity and are used in all industries and situations to handle a wide range of incidents.

There used to be 3 main categories

- Natural Disasters
- Physical Disasters
- Technology-Based Disasters

Now they need to cover incidents like:

- Natural disasters- fire, hurricanes, floods
- Technology is now tied to many things, Power outages, system failures, and Physical in most cases due to cameras, biometrics
- Physical threats Active shooter, explosions, break ins

Do you know who your CERT team is (Cyber Emergency Response Team)?

Who is the first call to make?

Who will be internal communication to employees? External to clients and the media?

How will that communication happen depending on the incident?

- i.e. no power, texting? Calling? Do you have all current cell phone numbers, your insurance POC Etc.?

What should your staff's expectations be for both temporary and permanent changes?

Does staff know how the transition of authority works with back ups for those people?

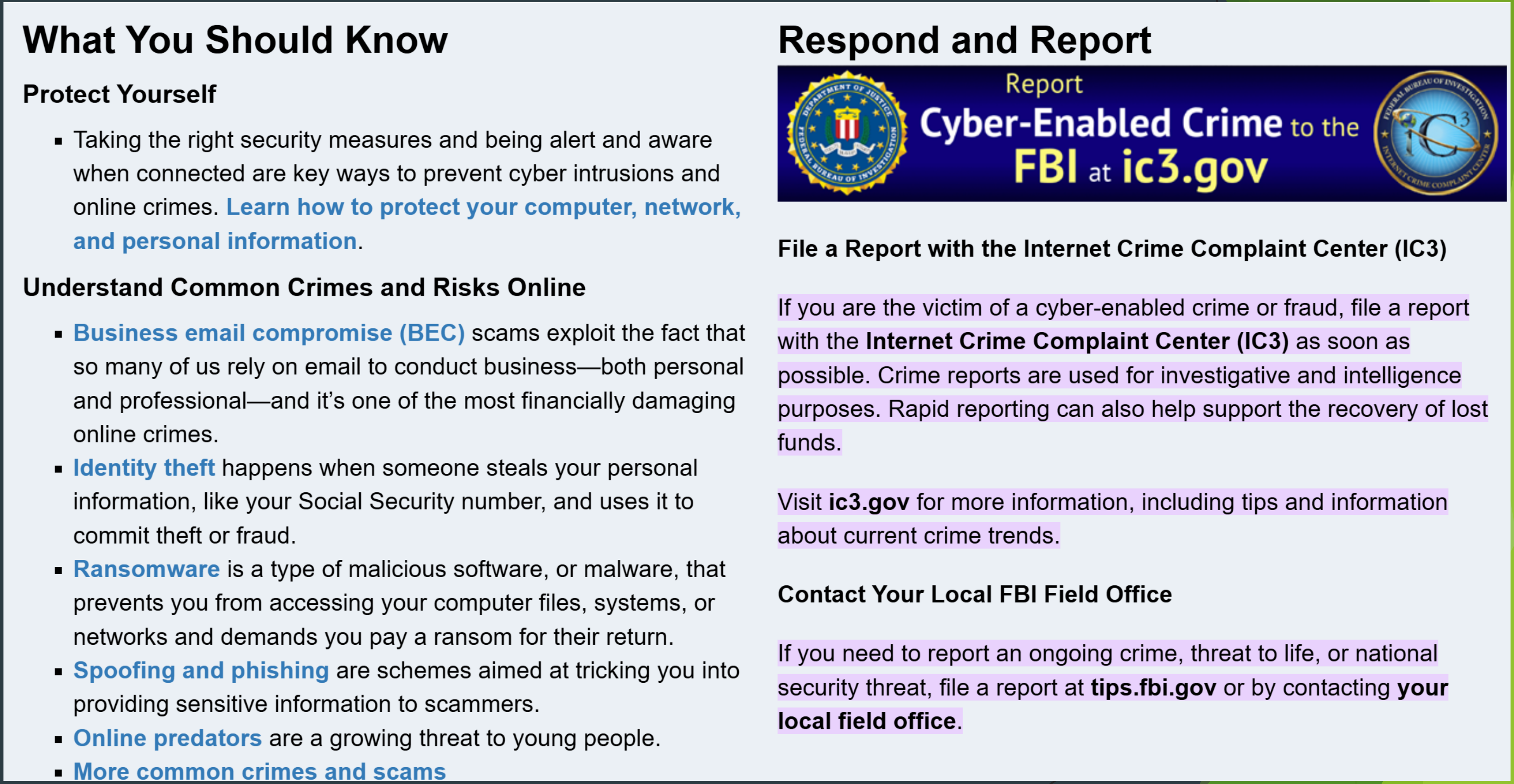
Do you have a business continuity plan in place with the most critical pieced of infrastructure?

Have you ever done an actual drill, how do you know it works?

Do you know the criteria of a cyber breach and when you have to report it to the Department of Homeland Security?

A “cyber incident” is defined as any critical infrastructure that includes incidents that cause loss of confidentiality, integrity or availability of an information system or network, or a serious impact on resiliency of operational systems and processes…

isn’t it all…



What You Should Know

Protect Yourself

- Taking the right security measures and being alert and aware when connected are key ways to prevent cyber intrusions and online crimes. **Learn how to protect your computer, network, and personal information**.

Understand Common Crimes and Risks Online

- **Business email compromise (BEC)** scams exploit the fact that so many of us rely on email to conduct business—both personal and professional—and it's one of the most financially damaging online crimes.
- **Identity theft** happens when someone steals your personal information, like your Social Security number, and uses it to commit theft or fraud.
- **Ransomware** is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
- **Spoofing and phishing** are schemes aimed at tricking you into providing sensitive information to scammers.
- **Online predators** are a growing threat to young people.
- **More common crimes and scams**

Respond and Report

File a Report with the Internet Crime Complaint Center (IC3)

If you are the victim of a cyber-enabled crime or fraud, file a report with the **Internet Crime Complaint Center (IC3)** as soon as possible. Crime reports are used for investigative and intelligence purposes. Rapid reporting can also help support the recovery of lost funds.

Visit **ic3.gov** for more information, including tips and information about current crime trends.

Contact Your Local FBI Field Office

If you need to report an ongoing crime, threat to life, or national security threat, file a report at **tips.fbi.gov** or by contacting **your local field office**.

Do you have Jurisdictional Arrangements you would need to make?

Jurisdictional arrangements would be by notification to the Commonwealth of Virginia depending on the circumstance

National arrangements:

National Arrangements may require notifying FDA, FBI depending on the circumstances

Virginia

Virginia Code 18.2-186.6 and 32.1-127.1:05

Legislative Directive

The rapid increase in cybercrime has also resulted in the subsequent increase in cyber insurance claims.

Denial Rate:

40% of cyber insurance claims for 2024 were denied, due to noncompliance with their policy

Insurance is now commonly asking to see this

Many insurance companies, especially those specializing in cyber insurance, often require businesses to have a documented incident response plan.

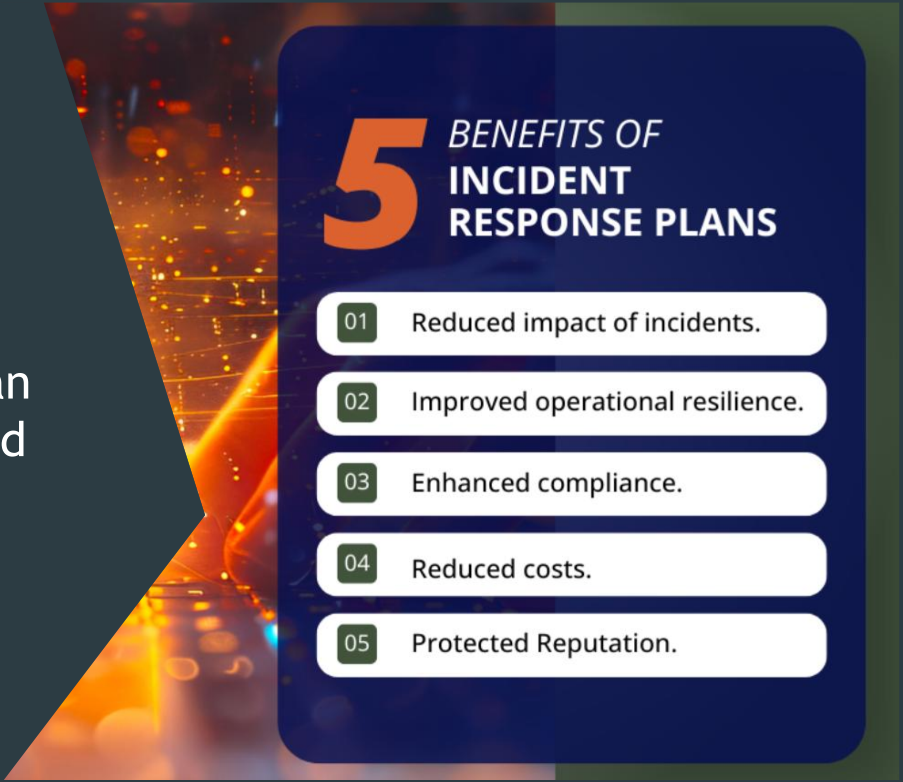
This is because a well-defined incident response plan can significantly reduce the financial impact of a cyberattack, making it easier for the insurance company to handle claims and for the insured to recover.

Ultimately your Incident Response Plan should be evolving and current.

It needs to be understood and accessible to all employees.

It needs to align with your insurance, compliance, and companies needs and someone needs to manage it against the policies, procedures and infrastructure in place.

The bottom line is an IR plan is critical and needs to work



5 *BENEFITS OF*
INCIDENT RESPONSE PLANS

01 Reduced impact of incidents.

02 Improved operational resilience.

03 Enhanced compliance.

04 Reduced costs.

05 Protected Reputation.