RICHEY MAY | Advisory

# CDSA Content Protection Summit 2021

## Ransomware Trends and Best-Practices


**Jason S. Hamilton, CISSP**

**Managing Director**

Cybersecurity Services

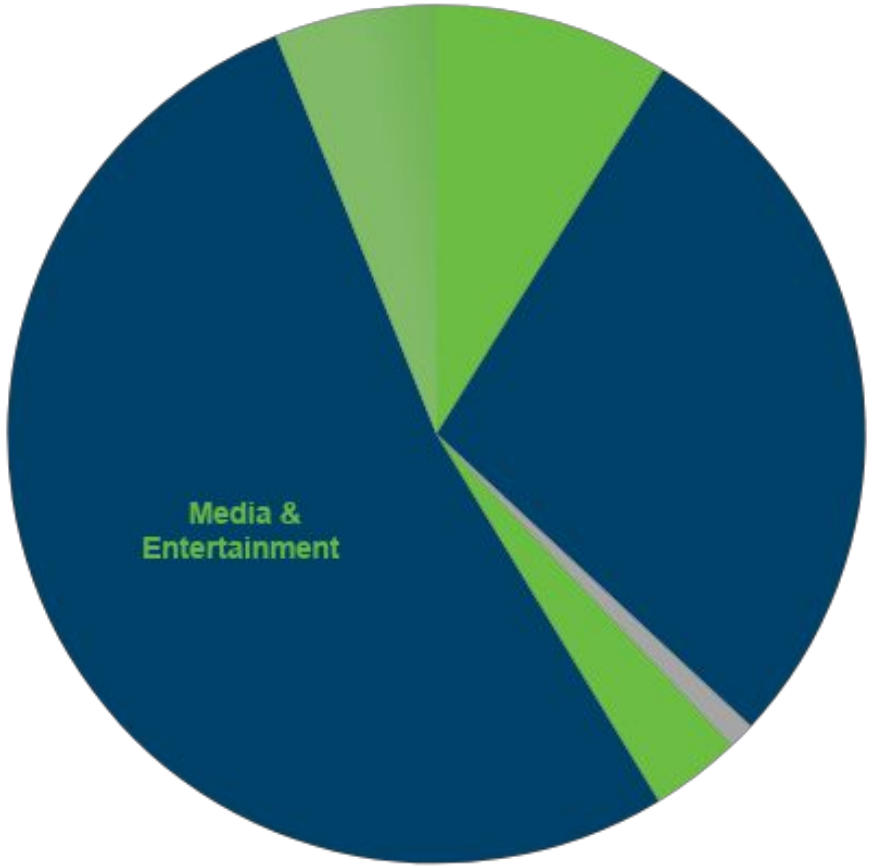
Richey May

# State of Cybersecurity

Today, the primary business for the majority of organizations is **INFORMATION.**

The Ponemon Institute reported Personally Identifiable Information (PII) is the costliest type of record to lose in a breach, at **$180** per record.*

The FBI IC3 identified **2,474** organizations in the United States impacted by Ransomware in 2020, with adjust losses of over **$29.1MM**.**



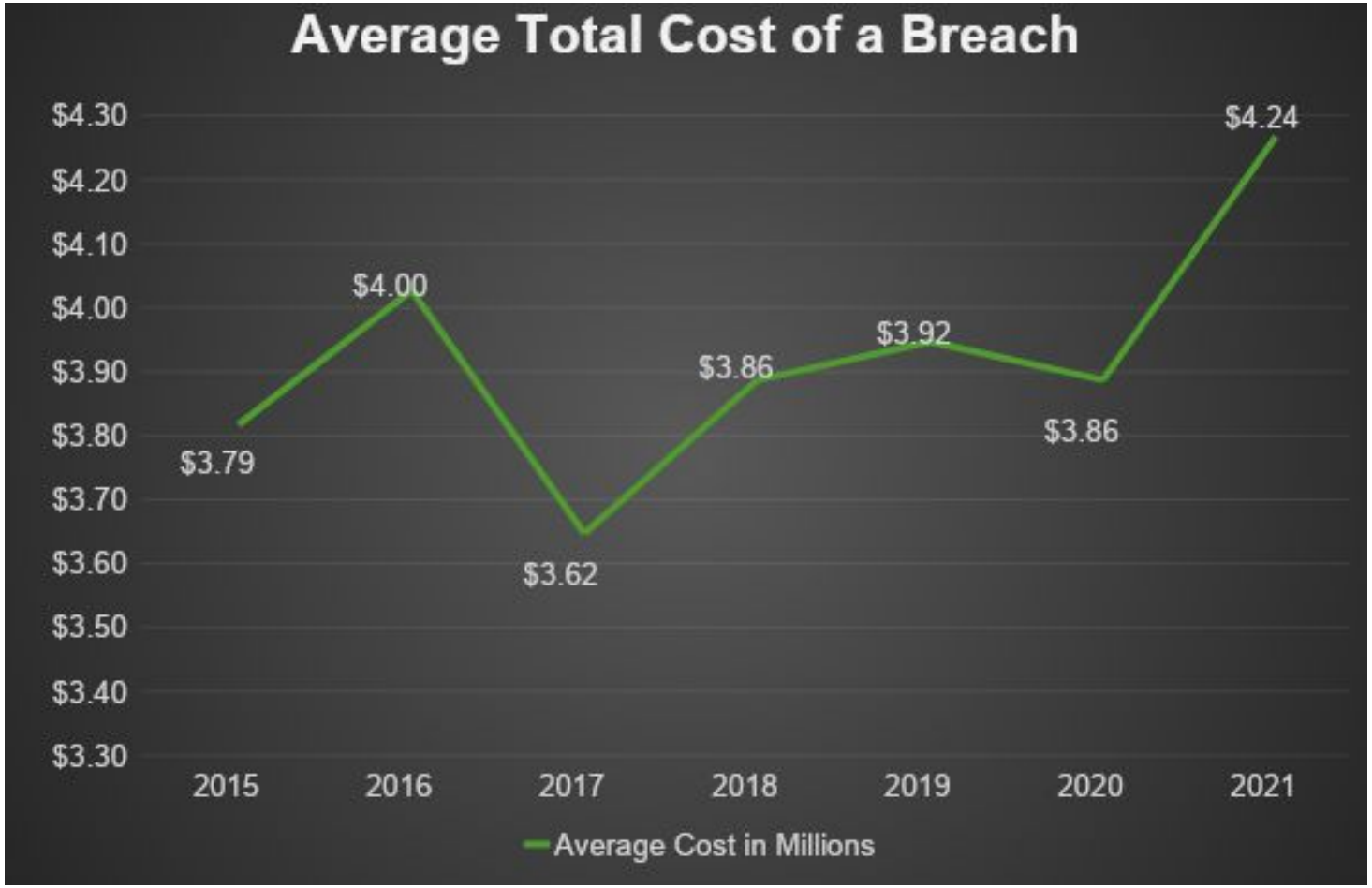

*IBM Cost of a Data Breach Report 2021 **2020 FBI IC3 Report

RICHEY MAY | Advisory

# State of Cybersecurity

The 2021 Verizon Data Breach Report found that costs associated with remediation of cyber incidents are also on the rise.

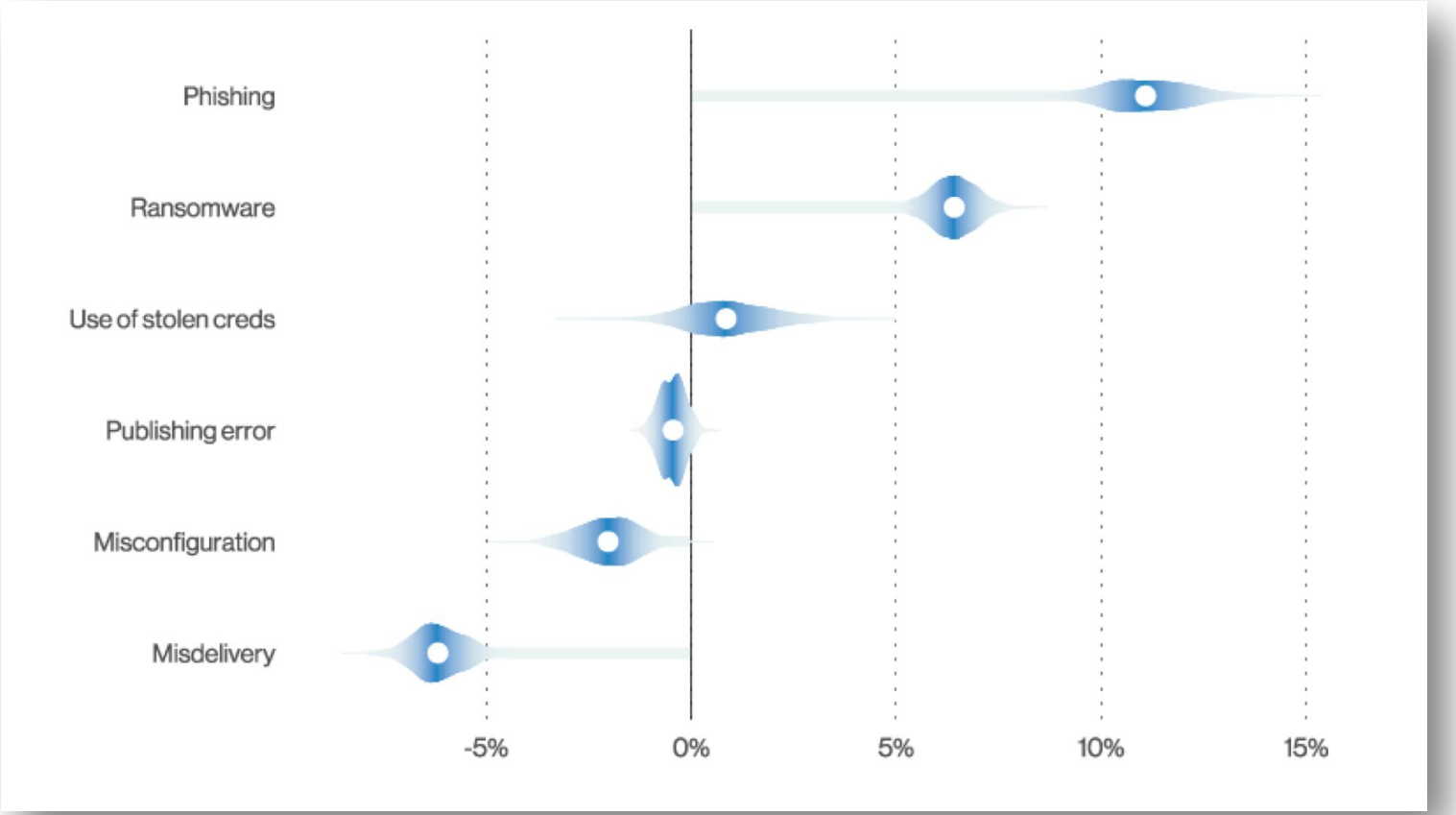
The Ponemon Institute finds the cost of a data breach has increased by **11.9%** since 2015, rising **$380,000** from 2020 to 2021.



# Remote Work Challenges

The average cost was **$1.07 million** higher in breaches where remote work was a factor in causing the breach.*

**Phishing** continues to be most prevalent attack vector, as it has for the last two years.




*IBM Cost of a Data Breach report 2021

RICHEY MAY | Advisory

# Current Threat Landscape

The **Window of Exposure (WoE)** metric represents the amount of time that an application has a serious vulnerability that can be exploited in a data breach.

## Window of Exposure (WoE)

Roughly **40% of Finance applications** have vulnerabilities with a WoE of more than **365 days**.

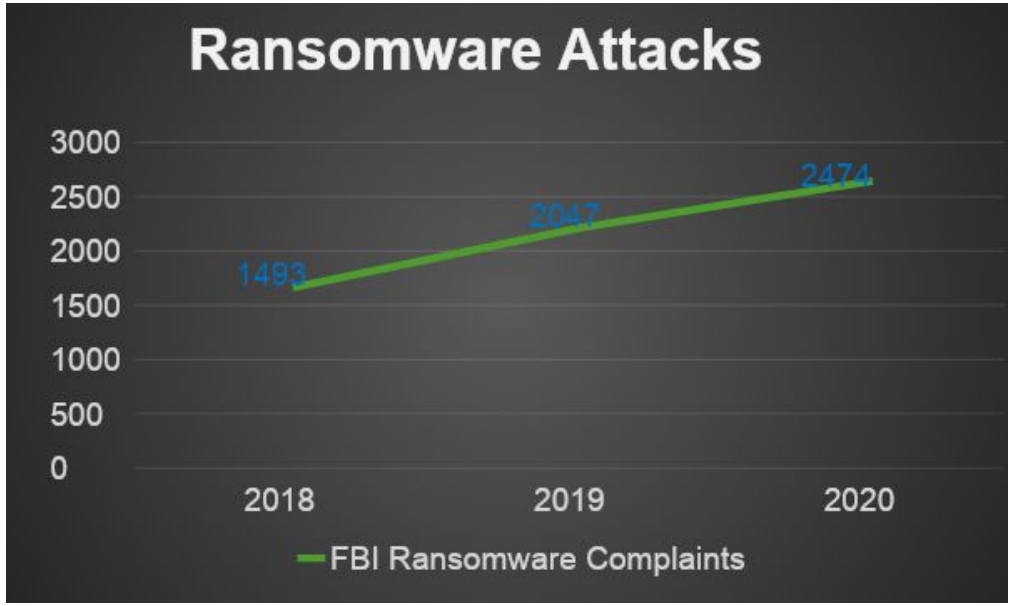
## The Mean Time to Remediate (MTTR)

A report from WhiteHat Security found by the end of June 2021, all industries took an average of **246 days** to fix high-severity vulnerabilities.

The Finance and Insurance industries average **286 days**.

# Current Threat Landscape

Cyber attacks are more sophisticated than ever, and criminal organizations are leveraging the same technology delivery models we use in legitimate business. **Ransomware as a Service (RaaS)** has already become a standard attack method.




The ransomware attack on **Colonial Pipeline** in 2021 made national news when it resulted in a 6-day shutdown of fuel delivery to a large portion of the US. Although Colonial paid the ransom, they ultimately recovered normal operations by **restoring from their own data backups**.

RICHEY MAY | Advisory

# Ransomware Defense and Recovery In a Nutshell

**Proactive Defense**

- Incident Handling policies and procedures
- Ransomware Procedure
- Monitoring, Logging, and Alerting
- Backup Strategy – DR/BCP
- Restore Procedures and Testing
- Network Segmentation
- Segregation of Critical Resources

**Incident Handling**

- Isolate the infected endpoints
- Close attack vector & validate impacted resources
- Follow process to sanitize infected hosts
- Restore compromised data from backup
- Validate the restore process
- Ensure documented RPO and RTO are met
- Lessons Learned and Process Improvement

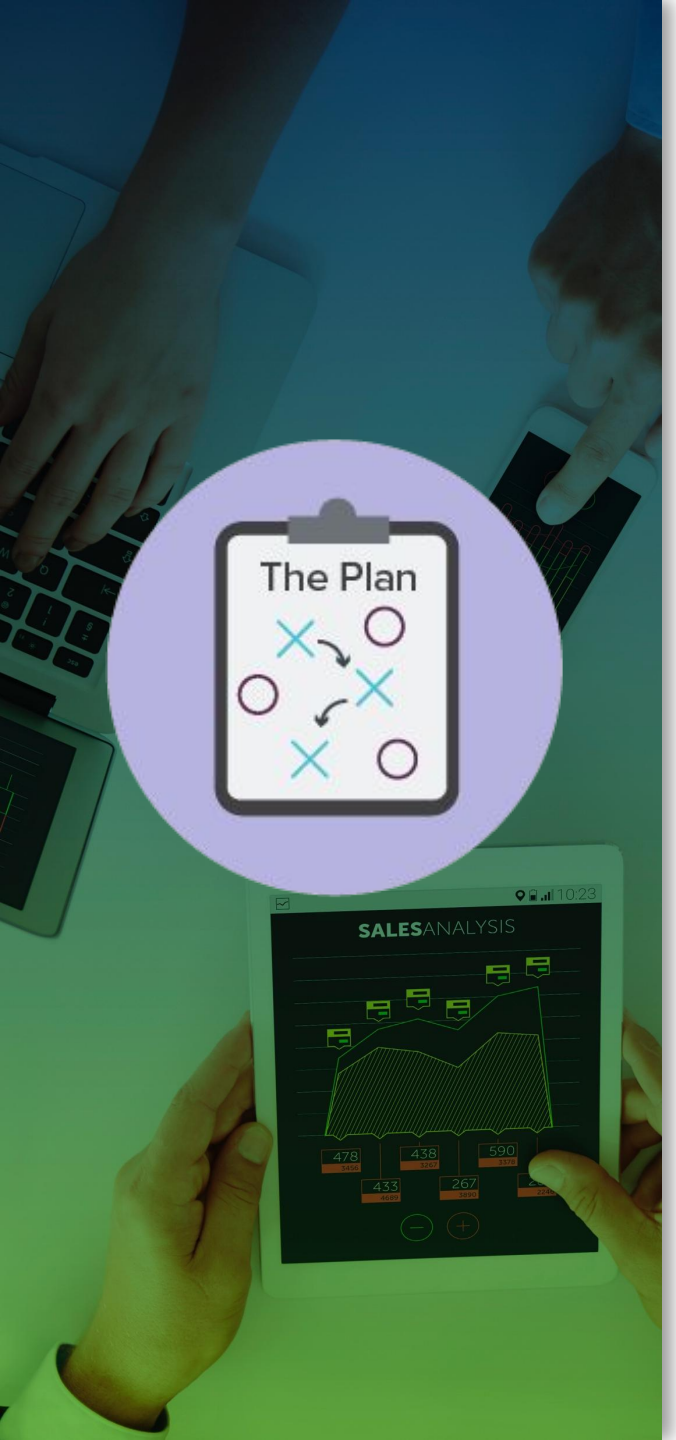
RICHEY MAY | Advisory

# Best Practices/Common Vulnerabilities

**Multi-factor Authentication is For Everyone.**

- Consider implementing Multi-Factor Authentication (MFA) for all remote access to your environment.
- MFA reduces the risk of users sharing passwords.
- MFA reduces the number of calls to your helpdesk for password resets.
- MFA reduces the ability of an attacker to compromise your platform remotely.

RICHEY MAY | Advisory




# Best Practices/Common Vulnerabilities

## Develop, Update, and Test your Incident Response Plan:

- **76% of companies** surveyed by Cisco admitted to not having an updated IR/DR strategy.
- Having a comprehensive plan can reduce your downtime as well as help you respond to a cyberattack such as ransomware.
- Include contacting the FBI early in the response plan.
- Develop Technology Solutions that are resilient by design.
- Develop a Pandemic Plan (define a taskforce and communication strategy)
- **Test your plan.**

RICHEY MAY | Advisory


# Best Practices/Common Vulnerabilities

**Patch management is still one of the most important elements of security:**

- Your customers' sensitive information is on endpoint devices, including smartphones, laptops, desktops, and servers.
- Patching reduces the threat of malicious software negatively impacting your daily business operation and compromising your customers' NPI data.
- Patching is not just for Microsoft products, but also 3rd party software from vendors such as Oracle and Adobe.
- Many of the major cybersecurity incidents that occurred in 2017, including Equifax, were the result of inadequate patch management practices.

# Thank You!

## Jason S. Hamilton, CISSP

Managing Director, Cybersecurity Services

Jason is a *Certified Information Systems Security Professional (CISSP)* with more than two decades' experience supporting organizations in Governance, Risk, and Compliance management, security program development, regulatory audit preparedness, and secure solution design.

Jason resides in the rural town of Elizabeth, Colorado with his wife and their two children, and spends his spare time snowboarding, woodworking, building muscle cars in his workshop, and leading a local Cub Scout den.