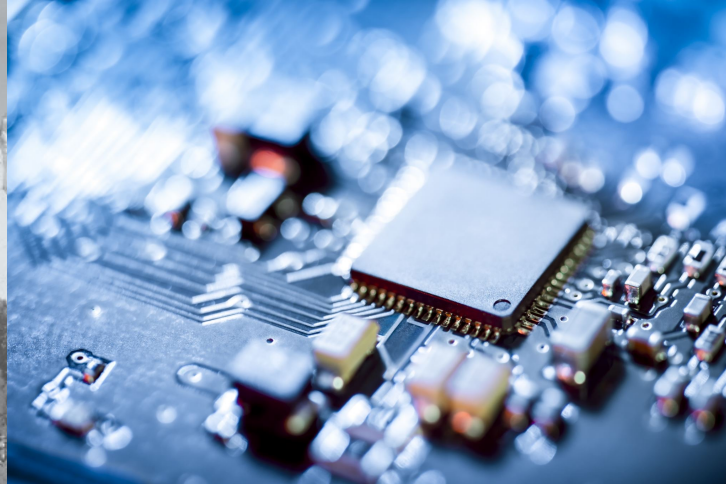




Discover / Develop / Deliver

## Unbreaking The Internet



## Our Presenter



### **Arnel Manalo, CISSP**

Director of Cybersecurity Services

Arnel Manalo is a Director of Cybersecurity Services with Richey May. Arnel has fourteen years of experience providing enterprise information technology, security and risk management services to a variety of organizations. He has been a Certified Information Systems Security Professional since 2014 and holds dual undergraduate degree in Computer Systems Security and Networking Technology from Colorado Technical University.



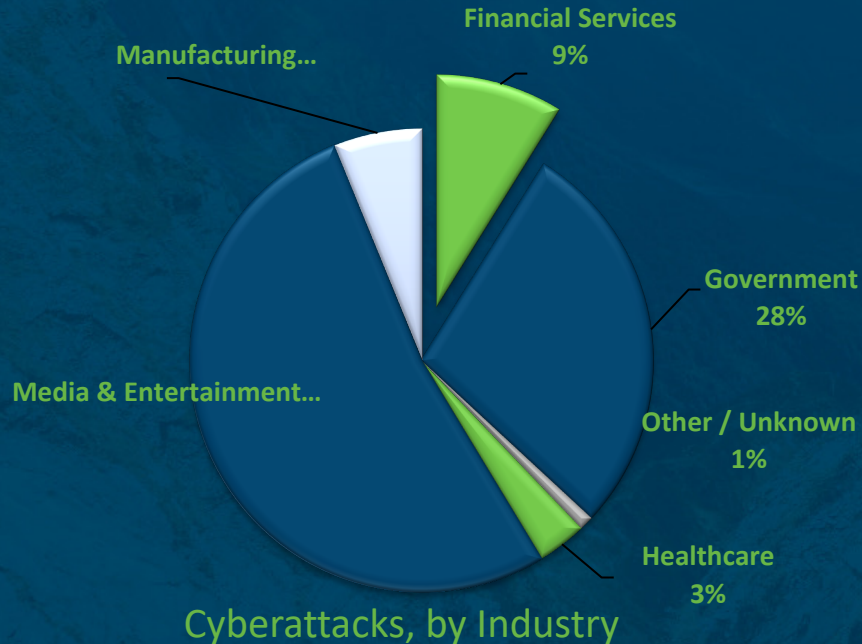
## About Us

Richey May Technology Solutions is a results-driven consulting firm offering the full spectrum of technology solutions for your business.

Led by technology experts with decades of cumulative experience in executive IT roles, our team is able to bring you pragmatic, real-world solutions that deliver value to your business.



## State of Cybersecurity – Before the Pandemic



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

The Ponemon Institute estimates that the average cost of remediation is **\$154** for every compromised customer record.

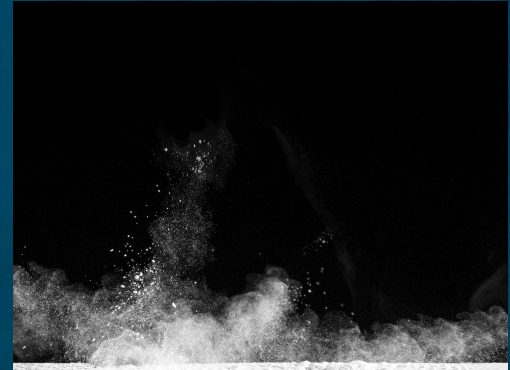
The FBI IC3 identified **2,474** organizations in the United States impacted by Ransomware in 2020.

\*2021 Verizon Data Breach Report. \*2020 FBI IC3 Report

## Industry Impact - Ransomware

---

- Funke Media Group (December 2020 – January 2021) – Ransomware on 6,000 laptops and thousands of additional endpoints halted production and caused them to remove the paywall on their website and only emergency issue papers released.
- Nine Entertainment (March 2021) – Ransomware locked out employees from emails, internet access and print production systems.



## Ransomware Defense

---

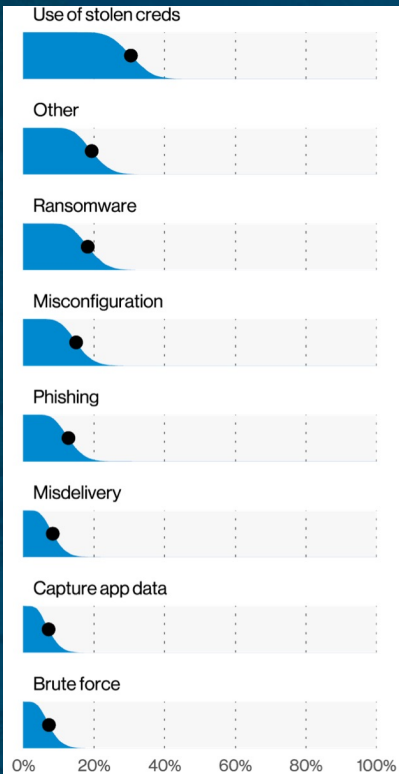
- User awareness and training.
- Perimeter defenses: AV/Malware detection on email, firewalls, IPS/IDS, etc.
- Endpoint defenses: AV/Malware, EDR/MDR
- Segmented and Distributed environment: Spread or segment critical systems to decrease impact of attack



# Industry Impact – Stolen Credentials

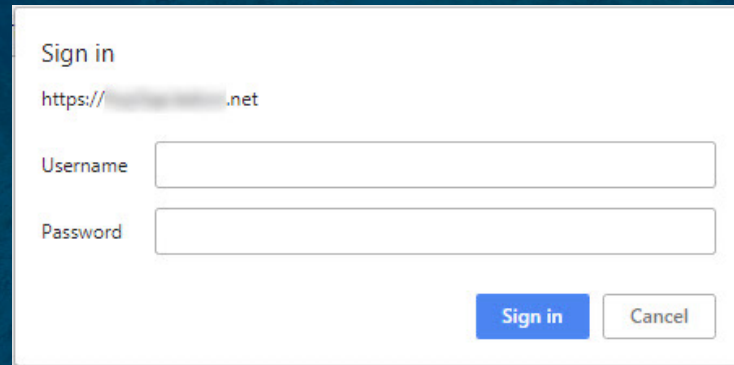
Among all the other threats to the industry, Stolen Credentials was the top cause of a data breach. “20% of the 88 billion total credential stuffing attacks observed during the reporting period targeted media companies.” (Akamai, 2020).

There are many ways to “hack” into systems; however, if an attacker has credentials, why try to hack something when you can just log in?



**Figure 100.** Top Actions in Arts and Entertainment breaches (n=90)

Source: Verizon DBIR 2021



Sign in

https://[redacted].net

Username

Password

## Stolen Credential Defense

---

- User awareness and training.
- Subscribe to known cracked password lists
- Enforce Multi-Factor Authentication
- Enforce behavioral, geographical, and suspicious login controls





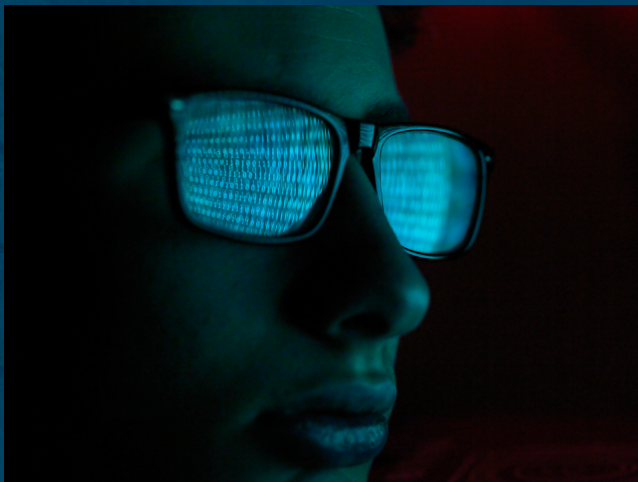
## Trusted Partner Network (TPN) Assessment

---

- Measurement on controls and maturity of the security program of a studio.
  - Segmentation of networks
  - Penetration Testing
  - Vulnerability Assessment
  - Patching and hardening assets
  - Change control
  - Policies and Procedures
  - Security Awareness
  - Many more...



## Penetration Testing vs Vulnerability Scanning



### **Penetration (Pen) Testing:**

Hired ethical hacker simulating real-life threats and LEVERAGES identified vulnerabilities and gaps within scope. Then provides a report on flaws and ways to remediate. Human interaction and hands on keyboard approach in addition to tools.

## Penetration Testing vs Vulnerability Scanning

---

### **Vulnerability Scanning:**

Automated scan from a tool of targets that produces a report based off vulnerabilities and ways to remediate. There is no leveraging or further testing to verify and validate fidelity of the findings.

---

In summary, the main differentiator is in a pen test, it is a simulated hacking exercise often much more complex and provides a step-by-step compromise report and recommendations to remediate along the way. Do not be sold on vendors providing a vulnerability scan claiming to be a pen test as these reports do not suffice to meet industry requirements.

## Additional Control – User Awareness

You may have noticed user awareness and training showed up in both ransomware and stolen credential defenses. No matter how many sophisticated tools, how well your networks are segmented, nor how hardened your devices are... there will always be a human element that adversaries can manipulate to gain access.



## Wrap Up

---

So what does this all mean? Cybercrime is increasing, because it is profitable. The more technology evolves and adapts, so do the criminals. Luckily, there is a force to fight these adversaries through following industry standards along with implementing proven tools and processes. We must remain diligent in being good stewards of content entrusted to us.



# Thank You.

[www.richeymaytech.com](http://www.richeymaytech.com)

Contact: Arnel Manalo

[arnel@richeymay.com](mailto:arnel@richeymay.com)