RICHEY MAY Technology Solutions

Discover / Develop / Deliver

Pirates of the Coronavirus: The Curse of Work from Home

RICHEY MAY Technology Solutions

Our Presenter

JT Gaietto, CISSP

Executive Director, Cybersecurity Services

JT Gaietto is the Executive Director of Cybersecurity Services with Richey May. JT has over twenty two years of experience providing enterprise information security and risk management services to a variety of organizations. He has been a Certified Information Systems Security Professional since 2003 and holds an undergraduate degree in Computer Information Systems from Northern Arizona University.

RICHEY MAY Technology Solutions

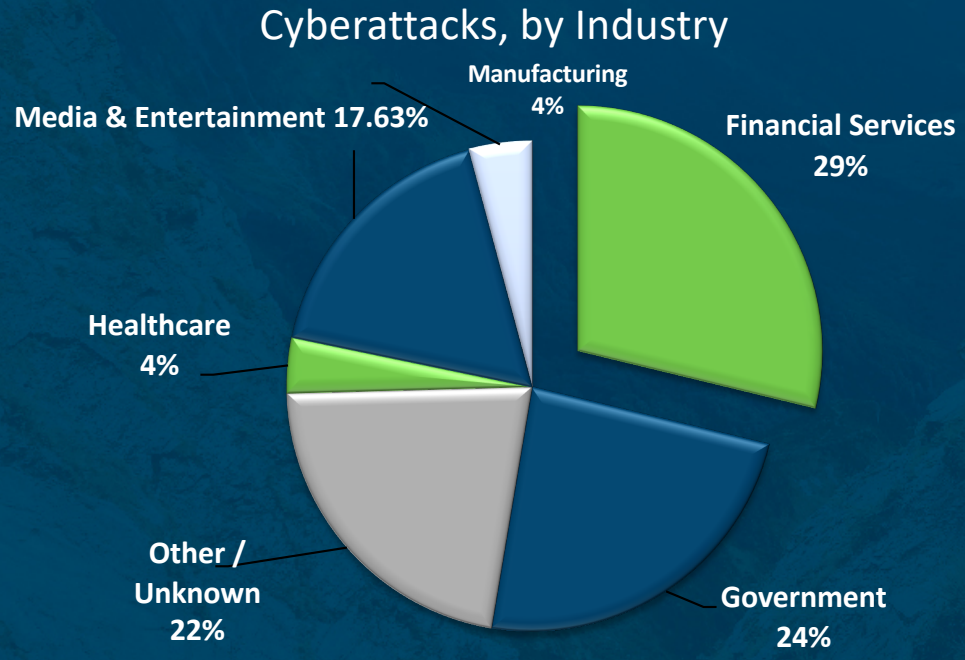
About Us

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.

RICHEY MAY Technology Solutions

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 **$150** for every compromised customer record.

The FBI IC3 identified **2,047** organizations in the United States impacted by Ransomware in 2019.

*2020 Verizon Data Breach Report

*2019 FBI IC3 Report

RICHEY MAY Technology Solutions

COVID-19 Challenges

- The COVID19 Pandemic has fundamentally changed the way companies operate
- Operations have become geographically disbursed, forcing new management and communications styles – technology teams needs to adjust to the new normal
- Employees not used to remote work have to adjust their mindset as well; anticipate the cultural shift in how people work, including how they handle creative content
- Front line managers must adjust their management style, and the technical tools are critical to managing those employees
- IT teams need to create systems that can support this new environment – and they **need to do it fast**, which often means **security is an afterthought,** and that's what can get you in trouble

RICHEY MAY Technology Solutions

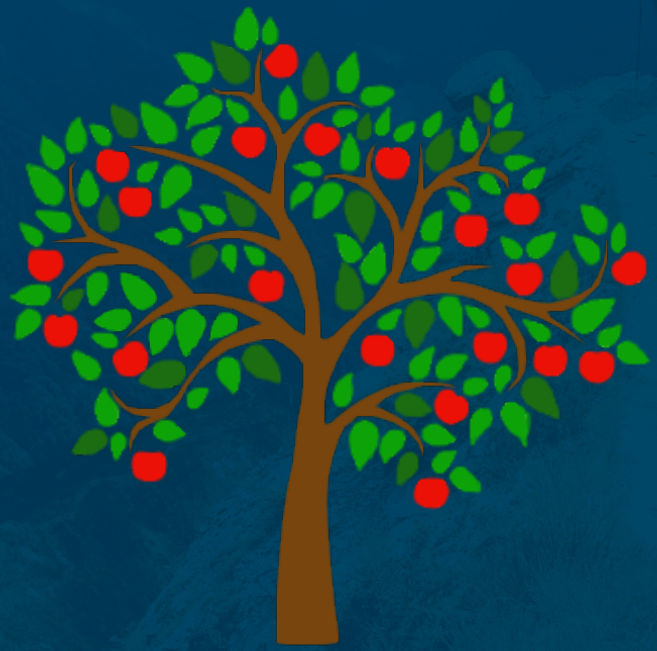
COVID-19 Challenges Increased Cybersecurity Risk

- FBI Notice on ZOOM.
- Calling the helpdesk asking for temporary credentials or a temp MFA token.
- Phishing emails around Covid-19 (false trackers, false information). Have you developed a formal communication strategy for your staff? (more on that in a moment)
- Malware designed around the fear, uncertainty and doubt caused by the shift to remote work.

RICHEY MAY Technology Solutions

Common Controls and Protections

Where should you be focused to reduce risk for your organization?



The following are several best practices recommendations that can have a meaningful impact.

RICHEY MAY Technology Solutions

MPA Best Practices November 2020

Monitoring the Remote Workforce

- Physical security of the employee's remote location, including door locks, alarms and surveillance camera systems.
- Employee remote locations should have separate networks with specific ACLs and controls to limit the upload and downloading of content. (Many companies are doing this via VPN).
- People at home are more likely to browse risky websites than in the office – make sure you can control this **EVEN OFF VPN.**
- The kids are home from school – are they plugging phones or drives into a corporate device? Can you block and detect this? Have you set the expectations?
- Is your remote infrastructure configured securely especially your VPN firewalls – do you scan for vulnerabilities, do all your users have local admin? are they using default admin credentials, especially the new ones you just built to send everyone home?

RICHEY MAY Technology Solutions

Additional Common Vulnerabilities

Remote User Support

- Your users are no longer physically present in the office. Are you validating they are who they say they are before resetting passwords or sharing sensitive information?
- Multi-Factor Authentication, like Frank's Red Hot. Use it on everything.
- Can you control devices remotely?
- How are you still distributing software and patches to the workstations?
- Do you have a standardized platform?
- Have you conducted an inventory of what your users have at home? Are you keeping track of what you've let them take home?

RICHEY MAY Technology Solutions

Piracy in 2020

What's changed?

Is it going up or down?

RICHEY MAY Technology Solutions

Piracy Over the Past Three Years

2017: Variety article outlines that nearly 40% of consumers did not care that piracy impacts the bottom line of content creators and artists

(https://variety.com/2017/digital/news/piracy-survey-consumers-studios-lose-money-1201961634/)

2018: A study completed by the European Union Intellectual Property Office Piracy and pirated content declines by 15%.

2019: The trend continues with the EUIPO finding that consumers accessed less pirated content down by 11%

(https://musically.com/2019/12/05/eu-study-reveals-music-has-seen-the-sharpest-decline-in-piracy/)

RICHEY MAY Technology Solutions

Piracy Trends in 2020

An article published by Diane Benjuya @ IBM mentions research completed by Hub Entertainment that found that similar to 2017 nearly 40% of consumers share their password to a streaming service, and do not consider it theft.

(https://securityintelligence.com/posts/account-fraud-killing-streaming-services-what-providers-can-do/)

Additionally Wired published an article essentially outlining how consumers could share their accounts “securely” with other individuals even those not part of their household.

(https://www.wired.com/story/share-online-accounts-without-sharing-password/)

RICHEY MAY Technology Solutions

Wrap Up

So what does this all mean? Aside from the economic impact, we're focusing on attacks and piracy models from the 1990s. While it continues to be important to safeguard content as it is made.

Most of the piracy now arguably comes from streaming service theft.

As we move into a new reality of streaming content being the primary source of revenue for companies, looking at more complex authentication methods, and audience monitoring will be key to protecting the integrity of content and revenue models of the future.

RICHEY MAY Technology Solutions

Thank You.

www.richeymaytech.com

Contact: JT Gaietto

jt@richeymay.com