Organizational Security Threats and Vulnerabilities

Kimberly Badia

Colorado State University Global

ITS425: Ethical Hacking and Penetration Testing

Dr. Ryan Averbeck

July 4, 2021

Table of Contents

Section 1

Vulnerabilities and Threats

What threats are new this year and which have become more prevalent?

- Cloud Vulnerability and Misconfiguration
- Artificial Intelligence Cyberthreats & Fuzzing
- Machine Learning Poisoning
- Social Engineering Attacks
- Deepfake

Figure 1. Adapted from *Fake Obama created using AI video tool* by BBC News, 2017 (https://www.youtube.com/watch?v=AmUC4m6w1wo). Copyright 2021 by BBC.

Why are these threats more common and why are they important?

- Less emphasis on security awareness
- Underfunded security teams
- Most leaks & attacks involve inside participation
- Average attacks cost over $11 million

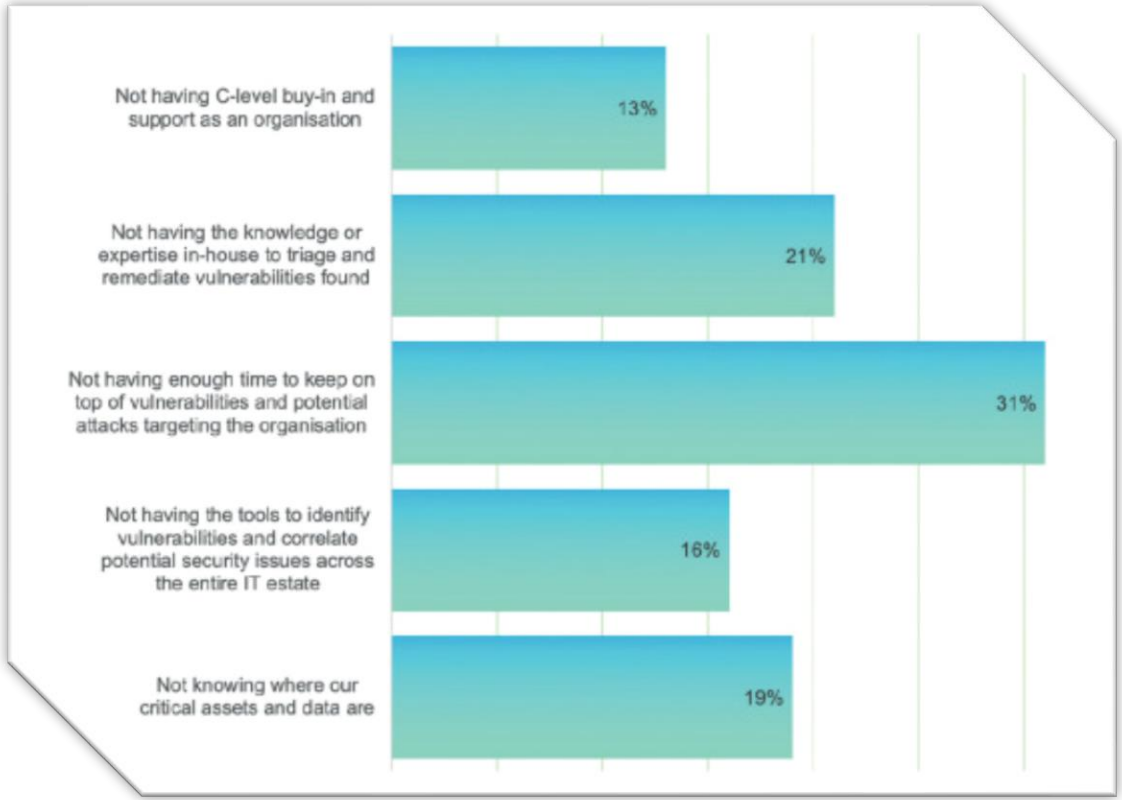


Figure 2. From *The 2020 Data Breach Investigations Report – a CSO's perspective* by Martin Jartelius, 2020 (https://www-sciencedirect-com.csuglobal.idm.oclc.org/science/article/pii/S1353485820300799). Copyright 2020 by Elsevier Ltd.

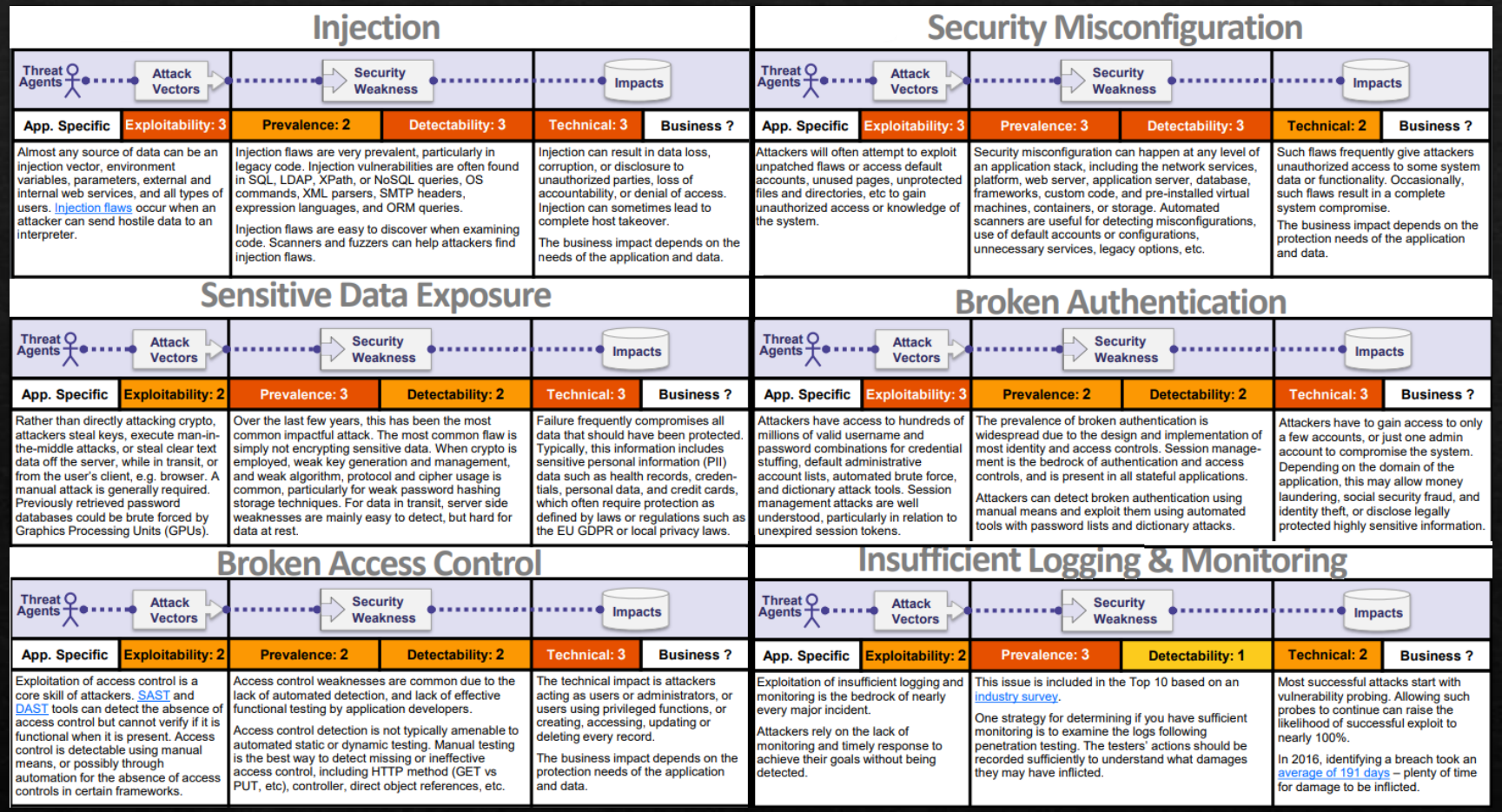


Figure 3. Adapted from *OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks* by OWASP Foundation, 2017 (file:///B:/klond_000/Downloads/OWASP%20Top%2010-2017%20(en).pdf). Copyright 2021 by OWASP Foundation, Inc..

What threats remain constant from year to year? Why?

- Injection Flaws
- Security Misconfiguration
- Sensitive Data Exposure
- Broken Authentication / Access Control
- Insufficient Logging & Monitoring

What threats do you believe will become more critical in the next 12 months? Why?

- Remote Working Means Higher Potential Exposure
- Ransomware Costs are Increasing
- Spear-Phishing Campaigns are More Sophisticated
- Covid-19 Created Pandemic-Related Security Problems
- More People Working Remotely Than Ever Before
- Cryptocurrency Decreases Risk to Cybercriminals

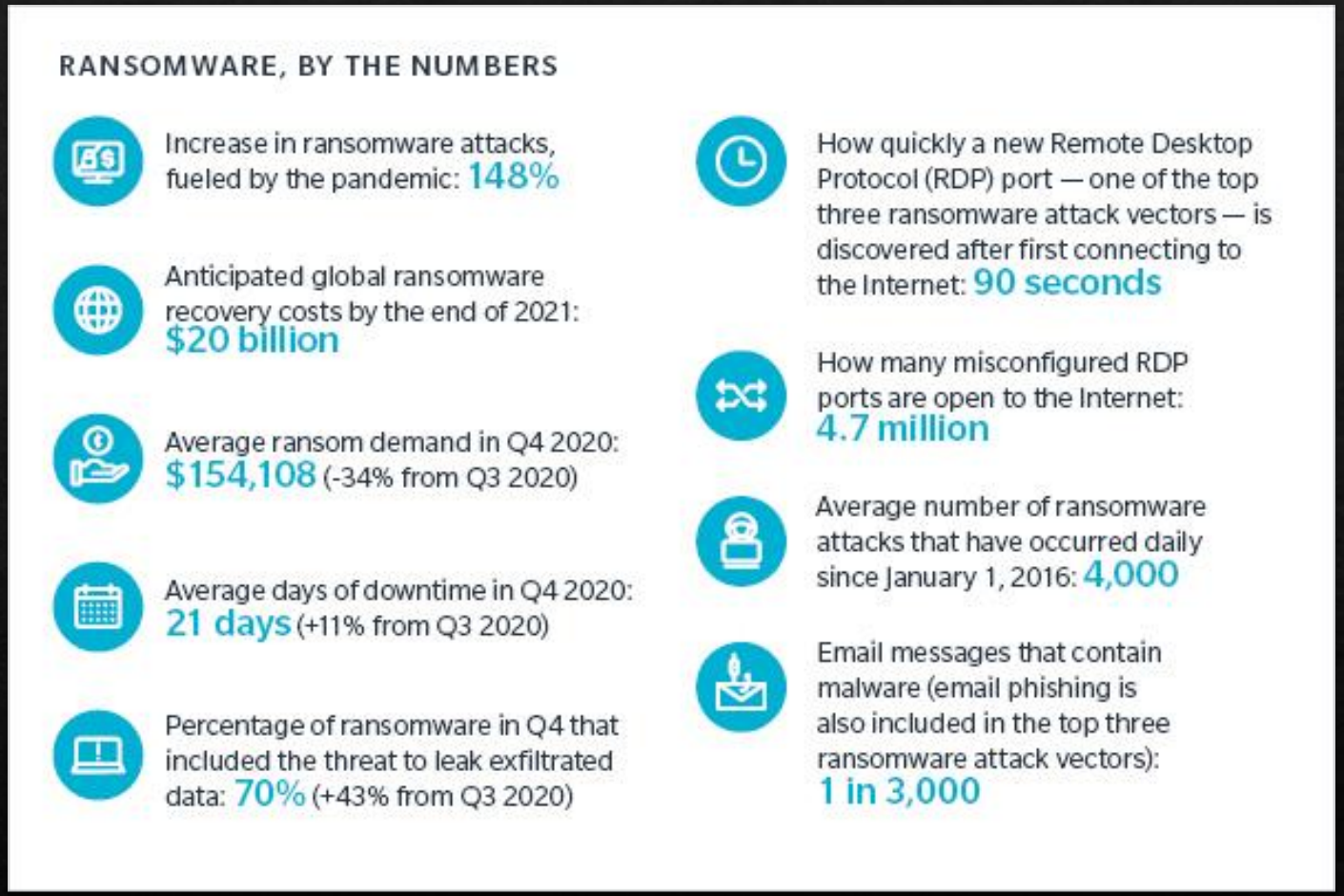


Figure 4. Adapted from *Ransomware Stats Every Business Needs to Know* by Marsh, 2021 (https://www.marsh.com/us/insights/research/ransomware-stats-every-business-needs-to-know.html)

Has an exploit been released?

- Critical Remote Code Execution(RCE) vulnerability
- Discovered and Published January 2021
- Current patches are easily bypassed
- Potentially exposes millions of corporate email accounts

Figure 5. Adapted from *Critical zero-day RCE in Microsoft office 365 awaits third security patch* by Adam Bannister, 2021 (https://portswigger.net/daily-swig/critical-zero-day-rce-in-microsoft-office-365-awaits-third-security-patch). Copyright 2021 by PortSwigger Ltd.

Figure 6. Adapted from *Corporate espionage is a lot closer than you may think* by Mark Raybin, 2015 (https://workingcapitalreview.com/2015/11/corporate-espionage-is-a-lot-closer-than-you-may-think/). Copyright 2021 by Working Capital Review.

What is the likelihood of an exploit?

- Assume Yes.
- Run deep antimalware scans
- Remove any existing malware
- Mandate all passwords be updated
- Verify inactive user accounts are deactivated

How widely used is the software or system?

- Public and Private Uses
- Student Lab Increases Exposure
- Web Servers
- Email Servers
- High Risk of Exposure

Section 2

Prevention and Countermeasures

Prevention is Key

- Proactive Identification
- Continuous Scanning
- Focus on raising staff security awareness
- Emphasis on cyber hygiene

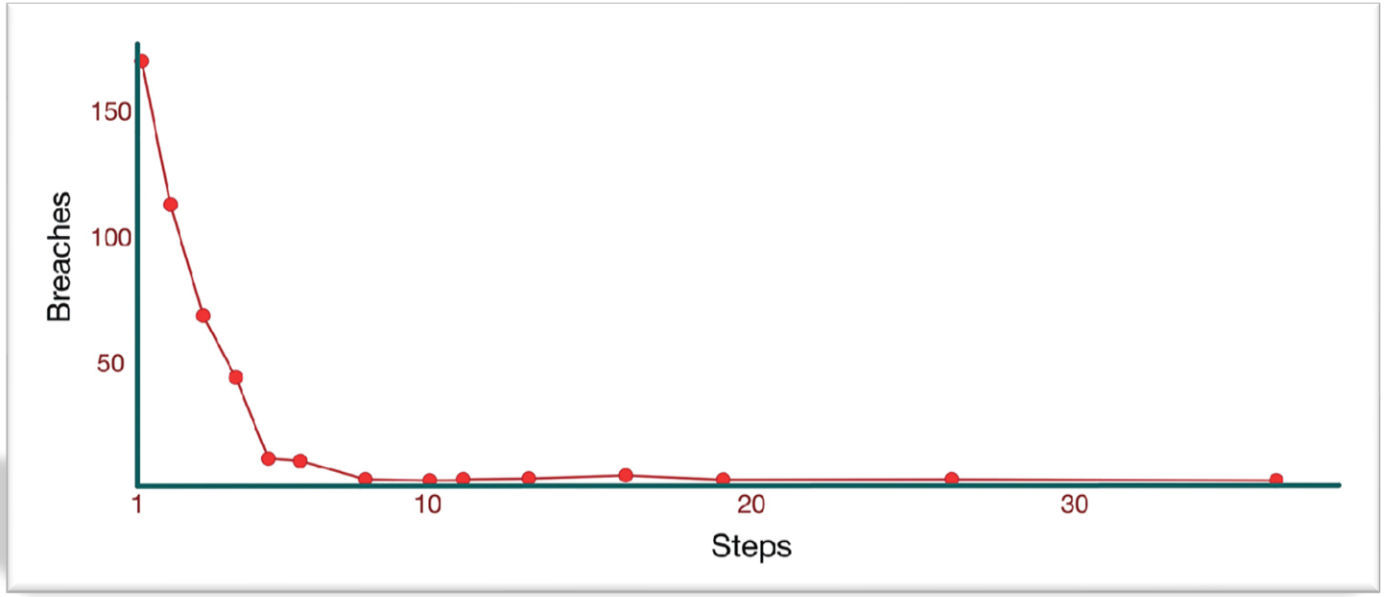


Figure 8. Adapted from *Why Misconfiguration Lead to Breaches - Cloud Security - Risk and Compliance* by Thom Bradley, 2020 (https://www.nsc42.co.uk/post/cloud-misconfiguration-leads-to-breaches). Copyright 2020 by NSC42 LTD.

Risk Mitigation

- Access Control – Least Privilege
- Regular system auditing
- Isolated Sensitive Data
- Updated Security Systems
- Active Triage and Remediation Protocols

Figure 9. Adapted from *Be proactive: Fight and mitigate future attacks with cyber threat hunting* by BankInfoSecurity, 2019 (https://www.bankinfosecurity.com/be-proactive-fight-mitigate-future-attacks-cyber-threat-hunting-a-12486).

Reducing Vulnerabilities Areas

Up-to-Date Security Systems

Strong Password Policies

Figure 10. Adapted from *10 ways to prevent computer security threats from insiders* by David Bianco, 2019 (https://searchsecurity.techtarget.com/feature/Ten-ways-to-prevent-insider-security-threats). Copyright 2021 by Tech Target.

Comprehensive, Regular Security Training

Risk Assessment

Figure 11. Adapted from *The importance of security awareness training* by S. Digital, 2016 (https://www.smarttech247.com/news/importance-security-awareness-training/). Copyright 2021 by SmartTech.

Counteracting an Active Attack: Incident Response

- Identify
  - Assets, Vulnerabilities, Risk Tolerance & Management
- Protect
  - Physical/Remote Access, Maintenance, CIA Triade
- Detect
  - Continuous Monitoring
- Respond
  - During & After the Incident, Mitigation
- Recover
  - System Restoration, Implement Improvements

Figure 12. From *The Five Functions* by NIST, 2021 (https://www.nist.gov/cyberframework). Copyright 2021 by National Institute of Standards and Technology, U.S. Department of Commerce.

Conclusion

The rate of cyber attacks is slightly decreasing, but the cost of a breach is skyrocketing – over 15% per annum on average.

New technologies are creating new methods for cybercriminals to attack systems including AI-based attacks to gain access to valuable information.

Addressing how to manage cybersecurity in a world where more people are working remotely than ever is imperative.

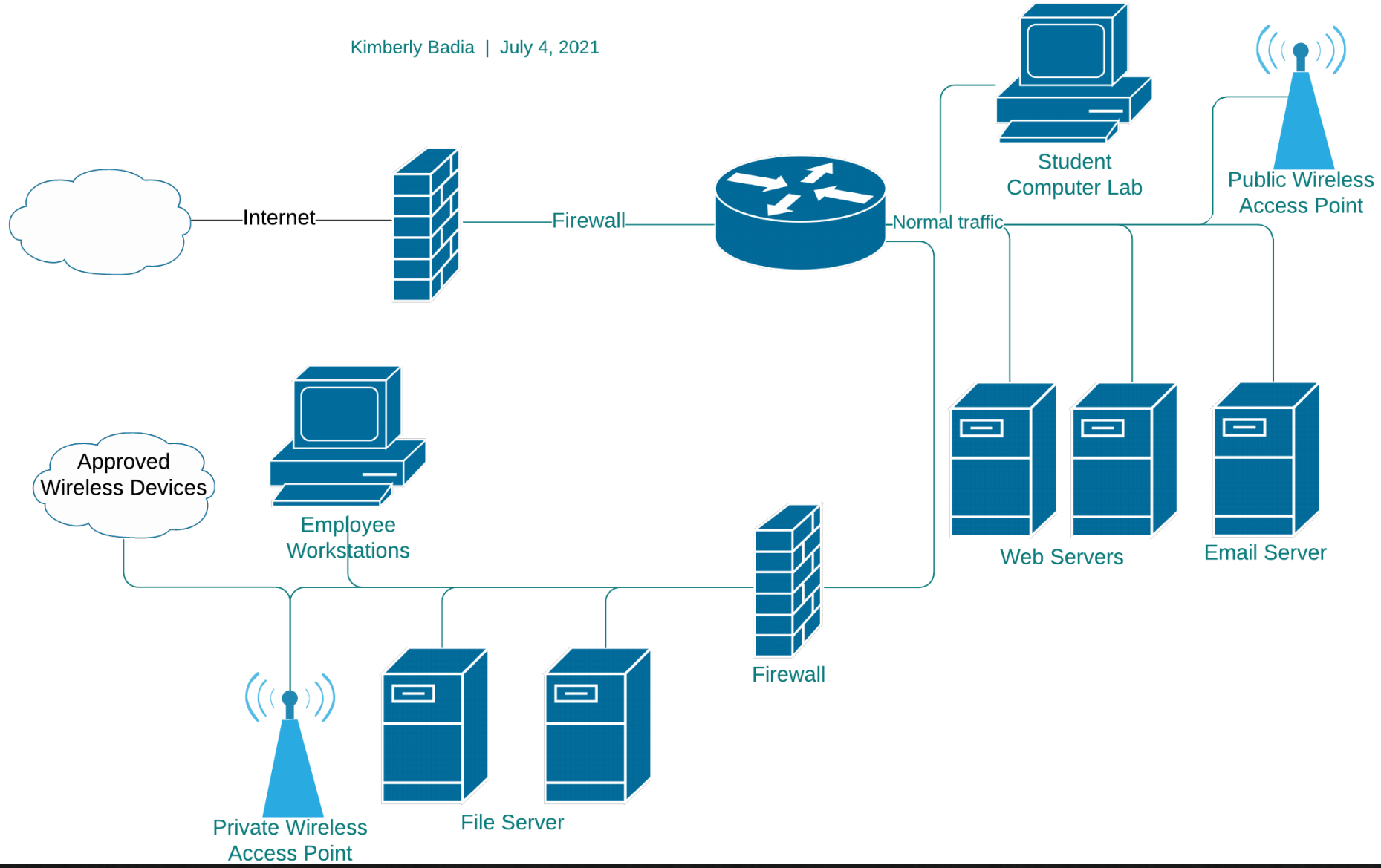
When a vulnerability cannot be eliminated, the risk must be mitigated or transferred when possible. If neither is feasible, additional resources for monitoring must be allocated.

Prevention and proactive vulnerability testing and elimination is infinitely preferable to reactive security measures

Having a comprehensive incident response plan in place prior to a breach can save millions in lost assets, customer and investor faith and prevent fines and penalties from leaked sensitive information.

Adventure Scuba and Diving Institute Network Diagram

Kimberly Badia | July 4, 2021



References

BankInfoSecurity. (2019, May 15). *Be proactive: Fight and mitigate future attacks with cyber threat hunting*. Bank information security news, training, education. https://www.bankinfosecurity.com/be-proactive-fight-mitigate-future-attacks-cyber-threat-hunting-a-12486

Bannister, A. (2021, January 13). *Critical zero-day RCE in Microsoft office 365 awaits third security patch*. The Daily Swig | Cybersecurity news and views. https://portswigger.net/daily-swig/critical-zero-day-rce-in-microsoft-office-365-awaits-third-security-patch

Belani, G. (2020, January 17). *5 cybersecurity threats to be aware of in 2020*. IEEE Computer Society. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020

Bradley, T. (2020, October 8). Why Misconfiguration lead to breaches - Cloud security - Risk and compliance. *Nsc42*. https://www.nsc42.co.uk/post/cloud-misconfiguration-leads-to-breaches

Hoske, M. (2020). Cybersecurity tips: Cybersecurity advice about process, technologies, people (internal) and external threat resulted from the Control Engineering 2020 Cybersecurity Research Report. *Control Engineering*, *67*(8), 16.

References

Jartelius, M. (2020). The 2020 data breach investigations report – a CSO's perspective. *Network Security*, *2020*(7), 9-12. https://doi.org/10.1016/s1353-4858(20)30079-9

Lohrmann, D. (2020, December 11). *2020: The year the COVID-19 crisis brought a cyber pandemic*. Government Technology State & Local Articles - e.Republic. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html

Marsh. (2021, January 22). *Ransomware stats every business needs to know*. Marsh | Global Leader in Insurance Broking and Risk Management. https://www.marsh.com/us/insights/research/ransomware-stats-every-business-needs-to-know.html

NIST. (2020, September 23). *SP 800-53 rev. 5, security and privacy controls for info systems and organizations*. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

References

NIST. (2021, May 12). *Cybersecurity framework: The five functions*. National Institute of Standards and Technology. Retrieved May 24, 2021, from https://www.nist.gov/cyberframework/online-learning/five-functions

Oriyano, S. P., & Solomon, M. G. (2020). *Hacker techniques, tools, and incident handling* (3rd ed.). Jones & Bartlett Learning.

OWASP Foundation. (2018). *OWASP Top 10 - 2017: The ten most critical web application security risks*. https://owasp.org/www-project-top-ten/

Raybin, M. (2015, November 20). *Corporate espionage is a lot closer than you may think*. Working Capital Review. https://workingcapitalreview.com/2015/11/corporate-espionage-is-a-lot-closer-than-you-may-think/