Strategies of Ethical Hacking and Penetration Testing

Adam Lee[1], Timothy Randhir[2]

1. Student: Springfield Technical Community College, Springfield, MA

2. Mentor: Professor, Springfield Technical Community College, Springfield, MA

Introduction

The digital age has brought up new issues and vulnerabilities to personal and professional information. With computers networked into almost every object, information is accessible anytime and anywhere. This access also allows outsiders to access without authorization. From 2014 to 2018, the total financial loss from cybercrime throughout the world increased from $8 million to $2.7 billion. The average cost of a data breach being $3.92 million in 2019 for a business, and an average of 279 days is spent to detect a breach. There is a need for proactive methods to prevent cybercrime. This study evaluates the use of ethical hacking to protect networks from cybercrime.

Objectives and Hypothesis

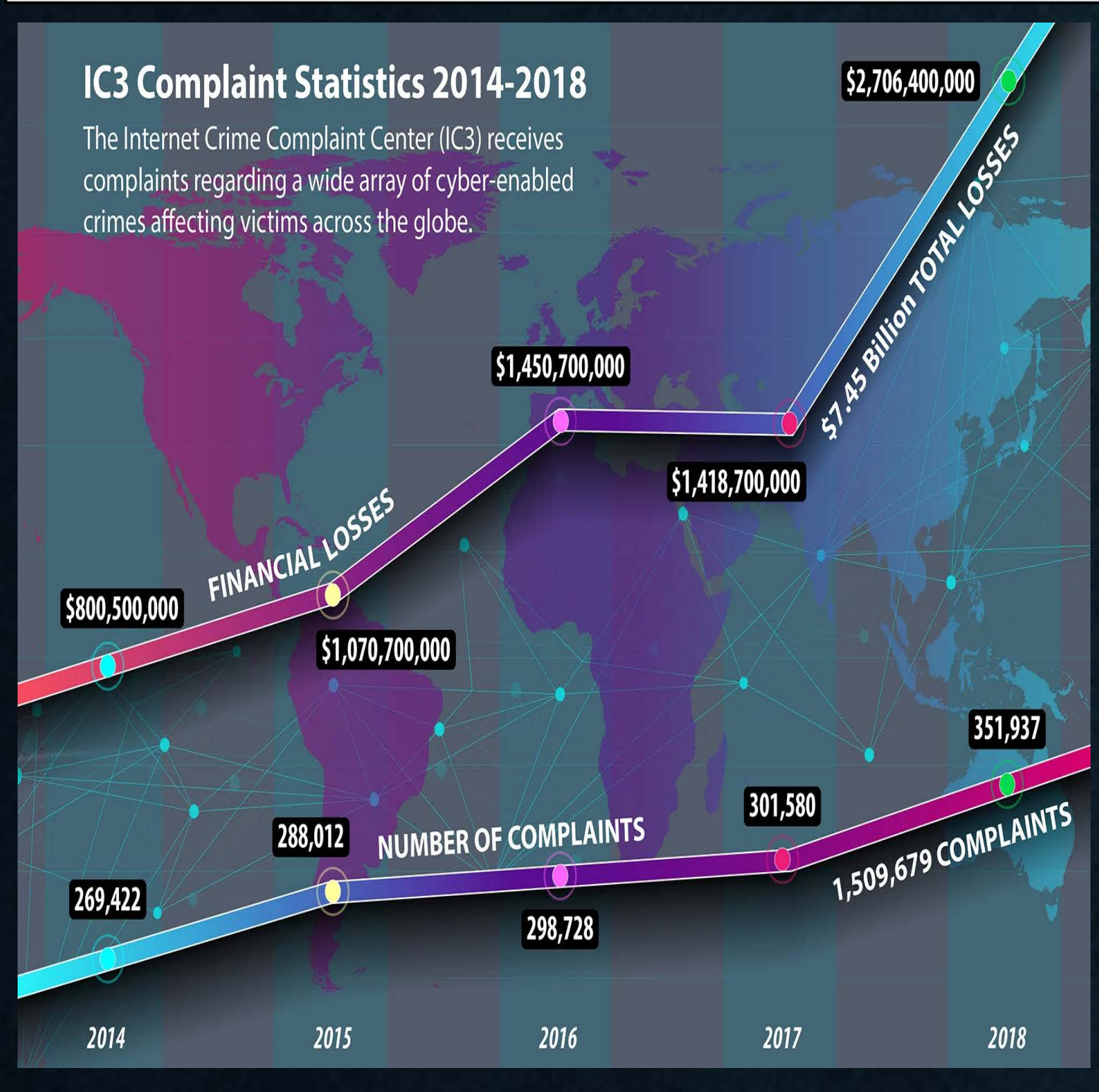
Aim: To assess the benefits of ethical hacking for use in preventing cybercrime

Specific:

1. To evaluate the trends in impact of cybercrime.
2. To assess the use of ethical hacking for deterring cybercrime.

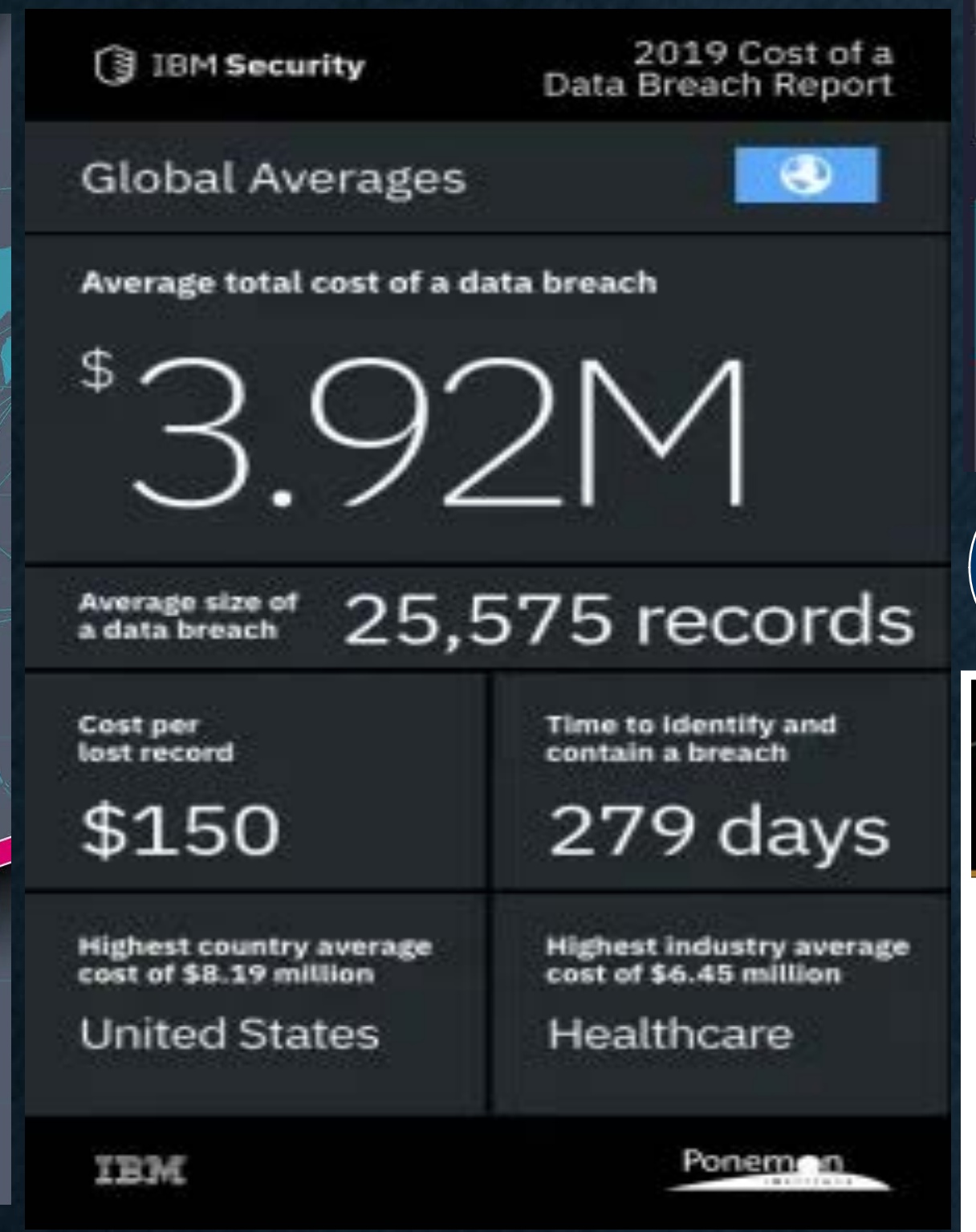
Hypothesis

1. Cybercrime continues to increase as new forms infiltration are invented.
2. Adding a proactive ethical hacking approach to find and fix vulnerabilities in a network can significantly reduce security breaches



IC3 Complaint Statistics 2014-2018

The Internet Crime Complaint Center (IC3) receives complaints regarding a wide array of cyber-enabled crimes affecting victims across the globe.



IBM Security — 2019 Cost of a Data Breach Report

Global Averages

Average total cost of a data breach: $3.92M

Average size of a data breach: 25,575 records

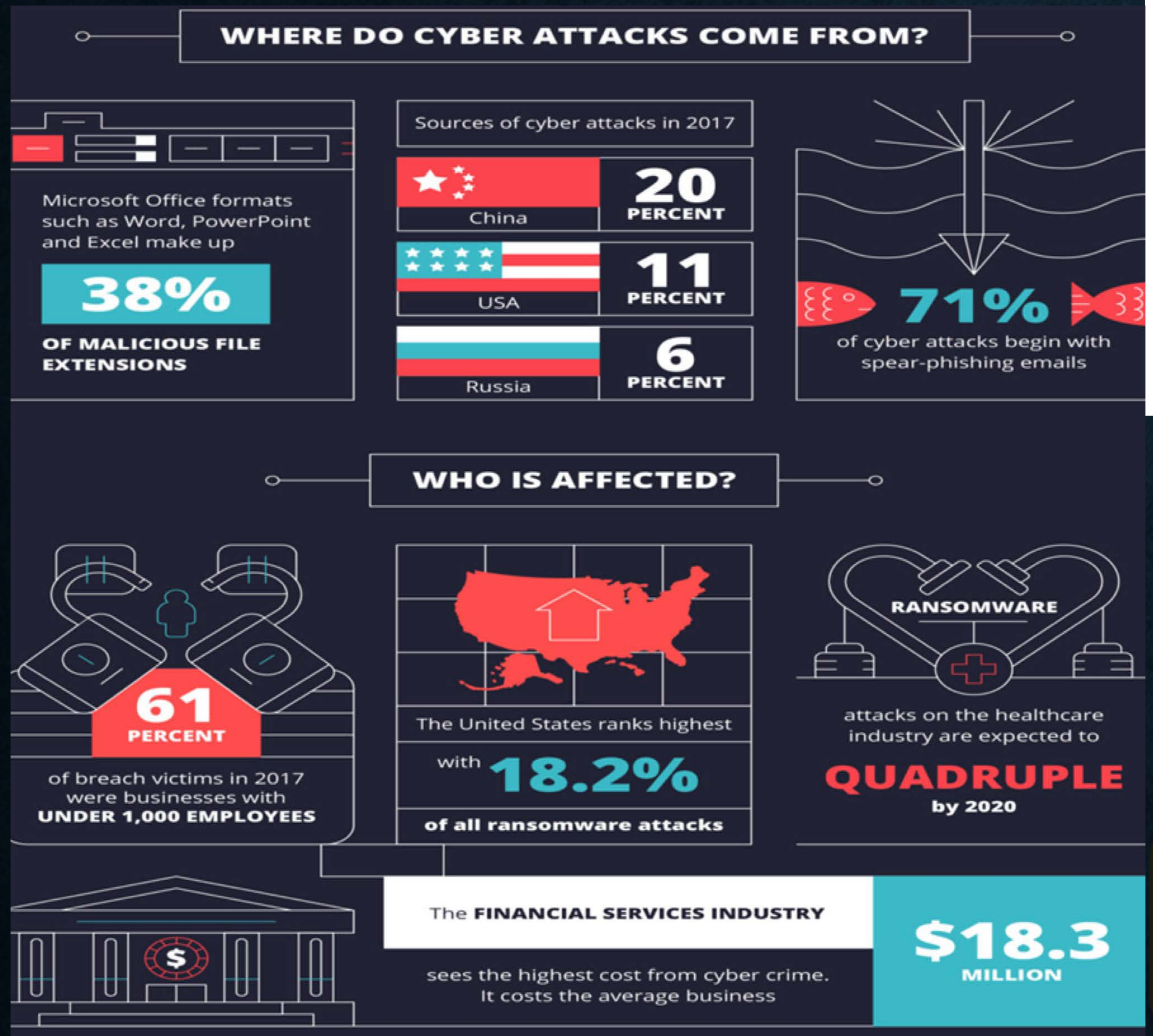
Cost per lost record: $150

Time to identify and contain a breach: 279 days

Highest country average cost of $8.19 million: United States

Highest industry average cost of $6.45 million: Healthcare

IBM — Ponemon



WHERE DO CYBER ATTACKS COME FROM?

Microsoft Office formats such as Word, PowerPoint and Excel make up 38% OF MALICIOUS FILE EXTENSIONS

Sources of cyber attacks in 2017

China	20 PERCENT
USA	11 PERCENT
Russia	6 PERCENT

71% of cyber attacks begin with spear-phishing emails

WHO IS AFFECTED?

61 PERCENT of breach victims in 2017 were businesses with UNDER 1,000 EMPLOYEES

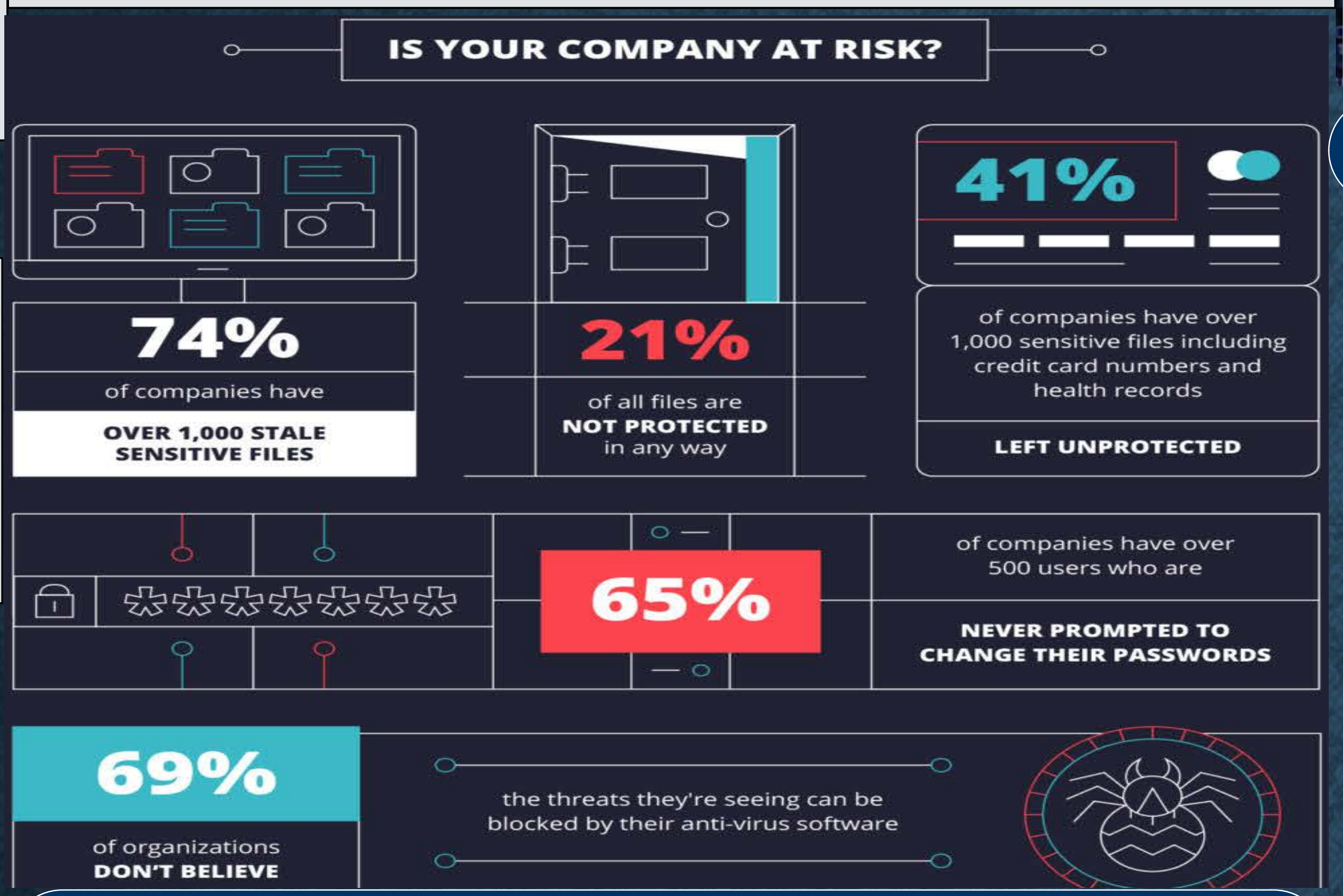
The United States ranks highest with 18.2% of all ransomware attacks

RANSOMWARE attacks on the healthcare industry are expected to QUADRUPLE by 2020

The FINANCIAL SERVICES INDUSTRY sees the highest cost from cyber crime. It costs the average business $18.3 MILLION

Methods

- ❑ A review of literature will be used to study the increase in cyber crime and to identify the potential of ethical hacking and penetration testing.
- ❑ Review the principle and theory of ethical hacking and determine pros and cons.
- ❑ Discuss how and why ethical hacking is an effective approach to deter cybercrime.



IS YOUR COMPANY AT RISK?

74% of companies have OVER 1,000 STALE SENSITIVE FILES

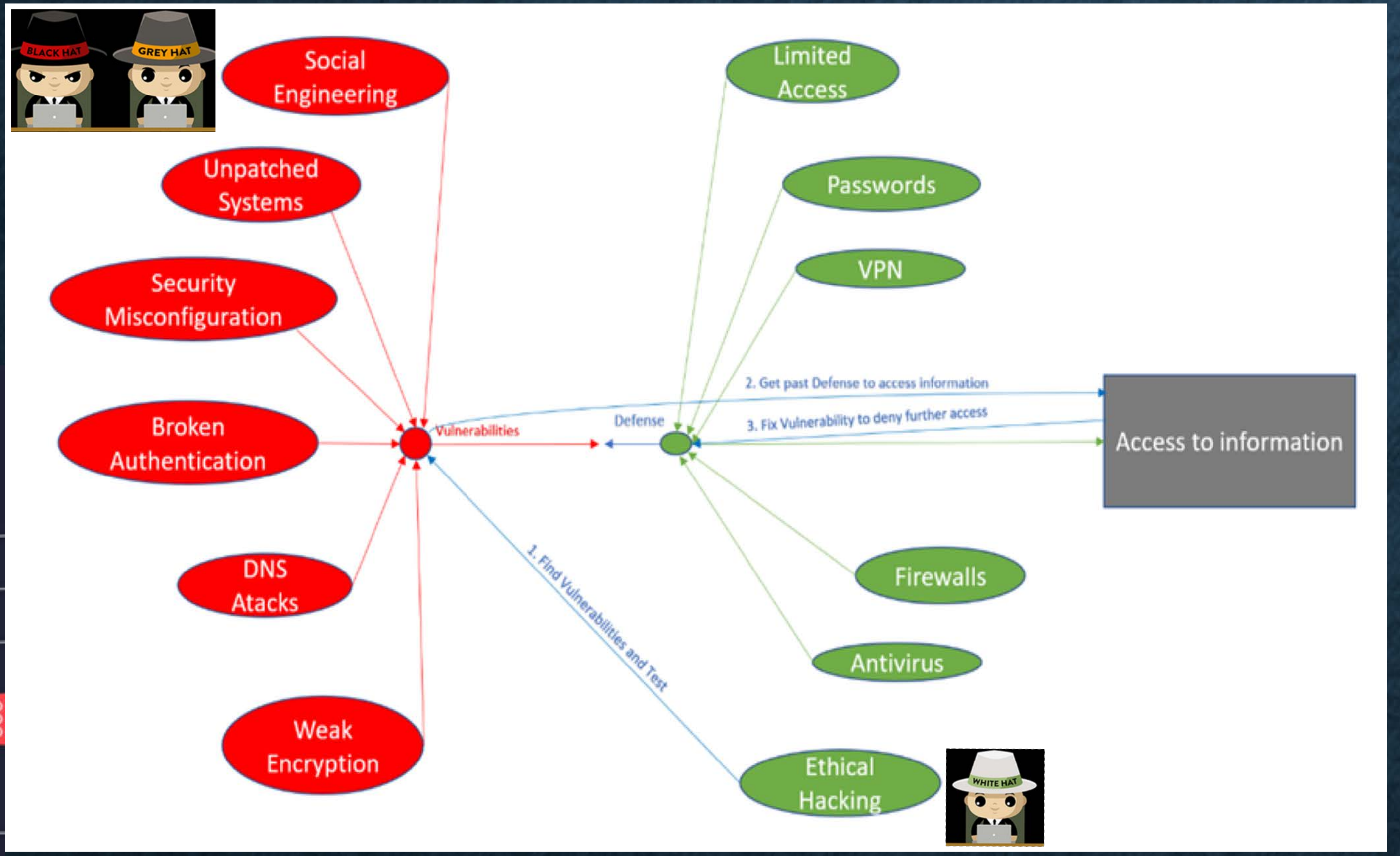
21% of all files are NOT PROTECTED in any way

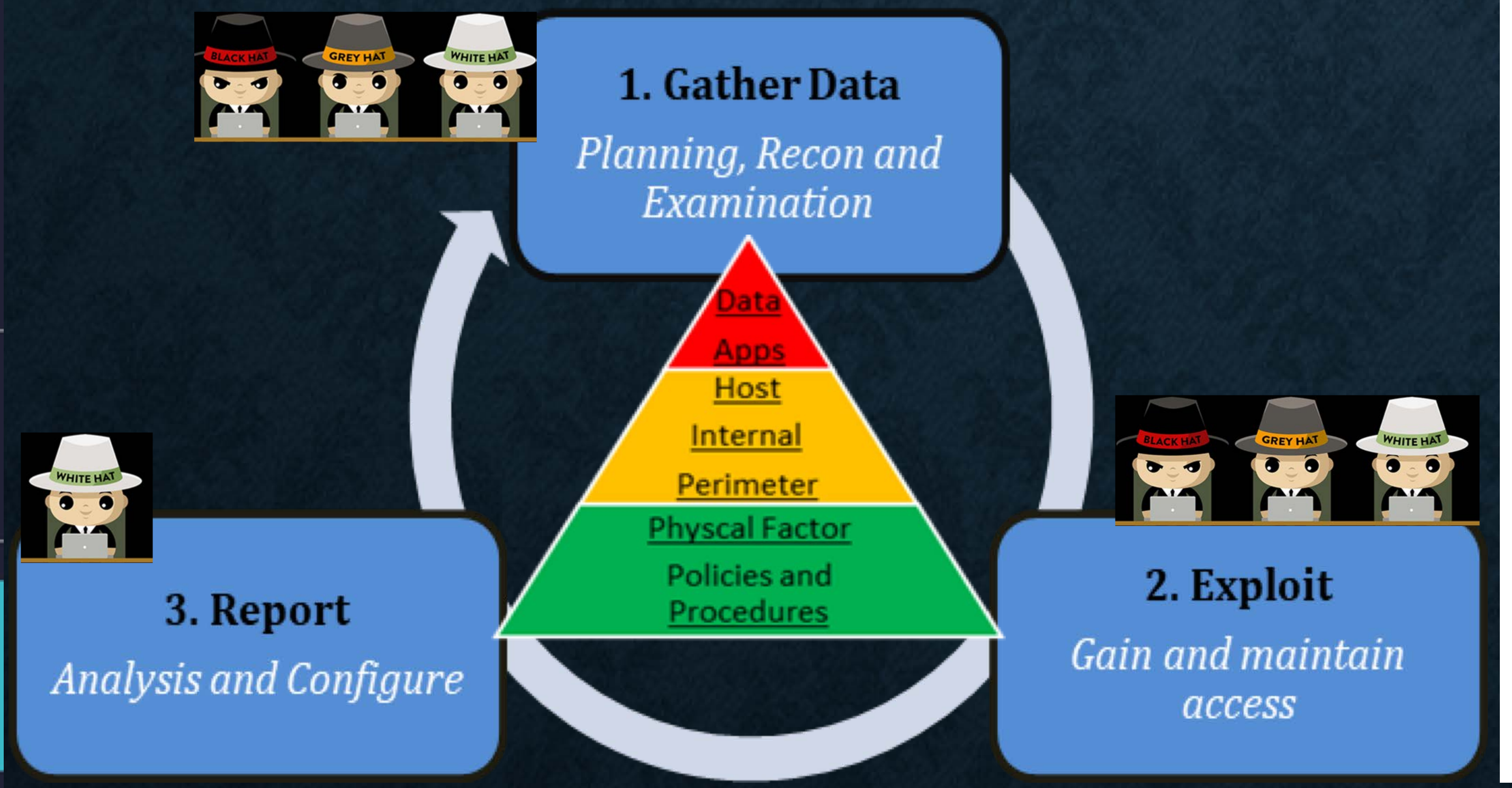
41% of companies have over 1,000 sensitive files including credit card numbers and health records LEFT UNPROTECTED

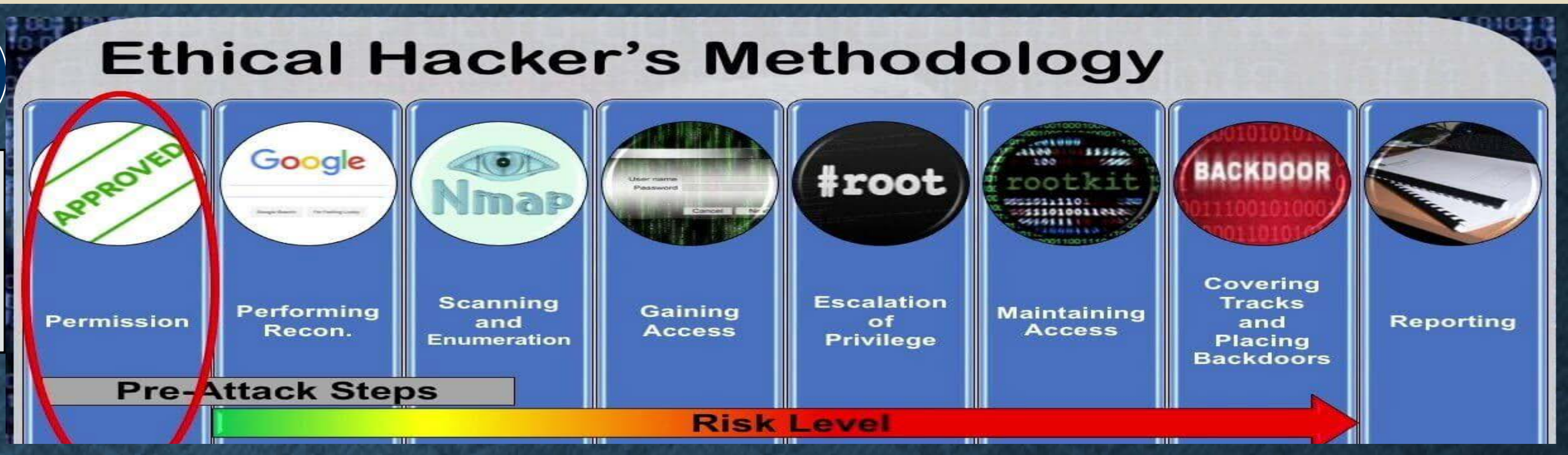
65% of companies have over 500 users who are NEVER PROMPTED TO CHANGE THEIR PASSWORDS

69% of organizations DON'T BELIEVE the threats they're seeing can be blocked by their anti-virus software

Conceptual model

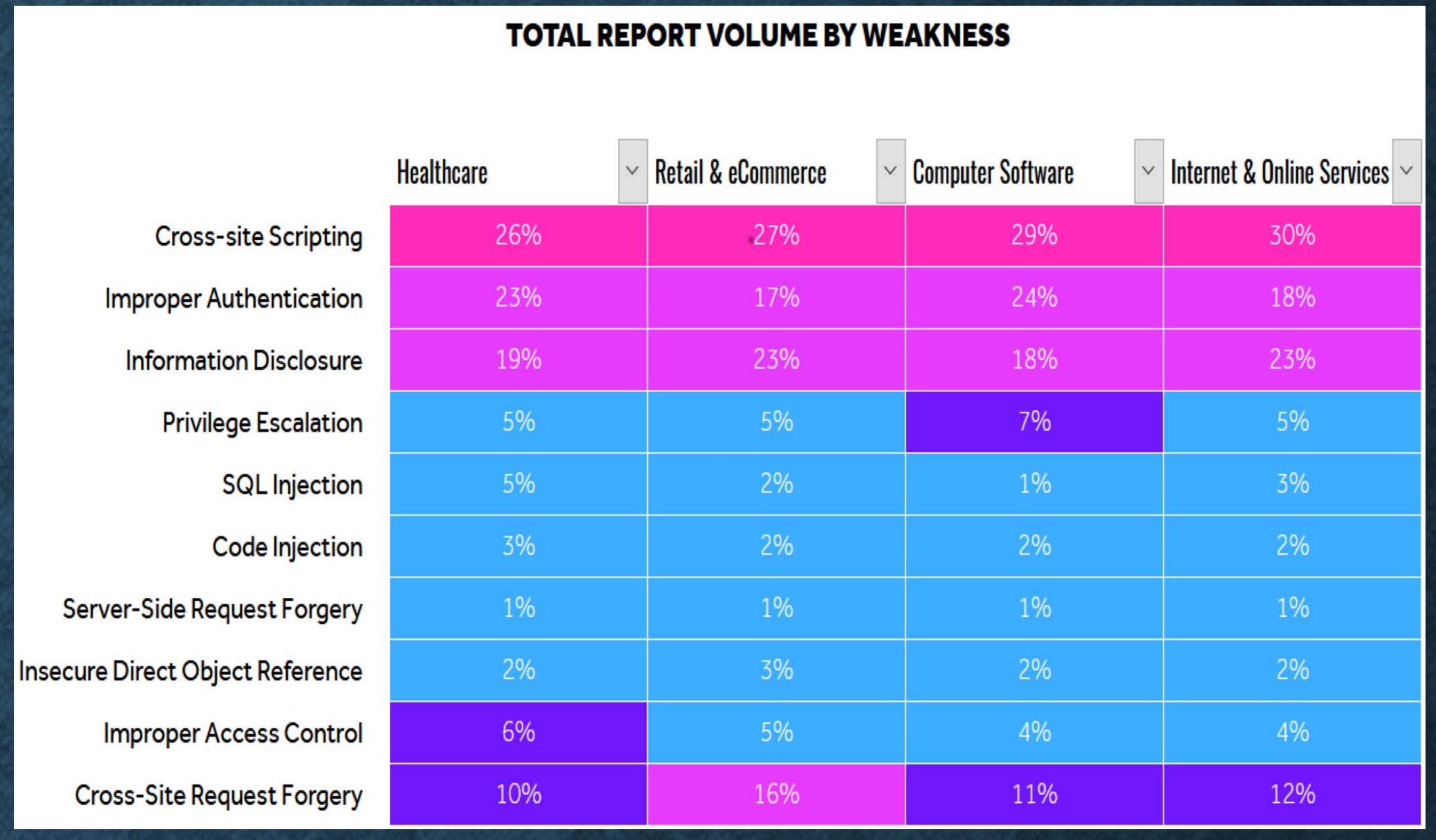






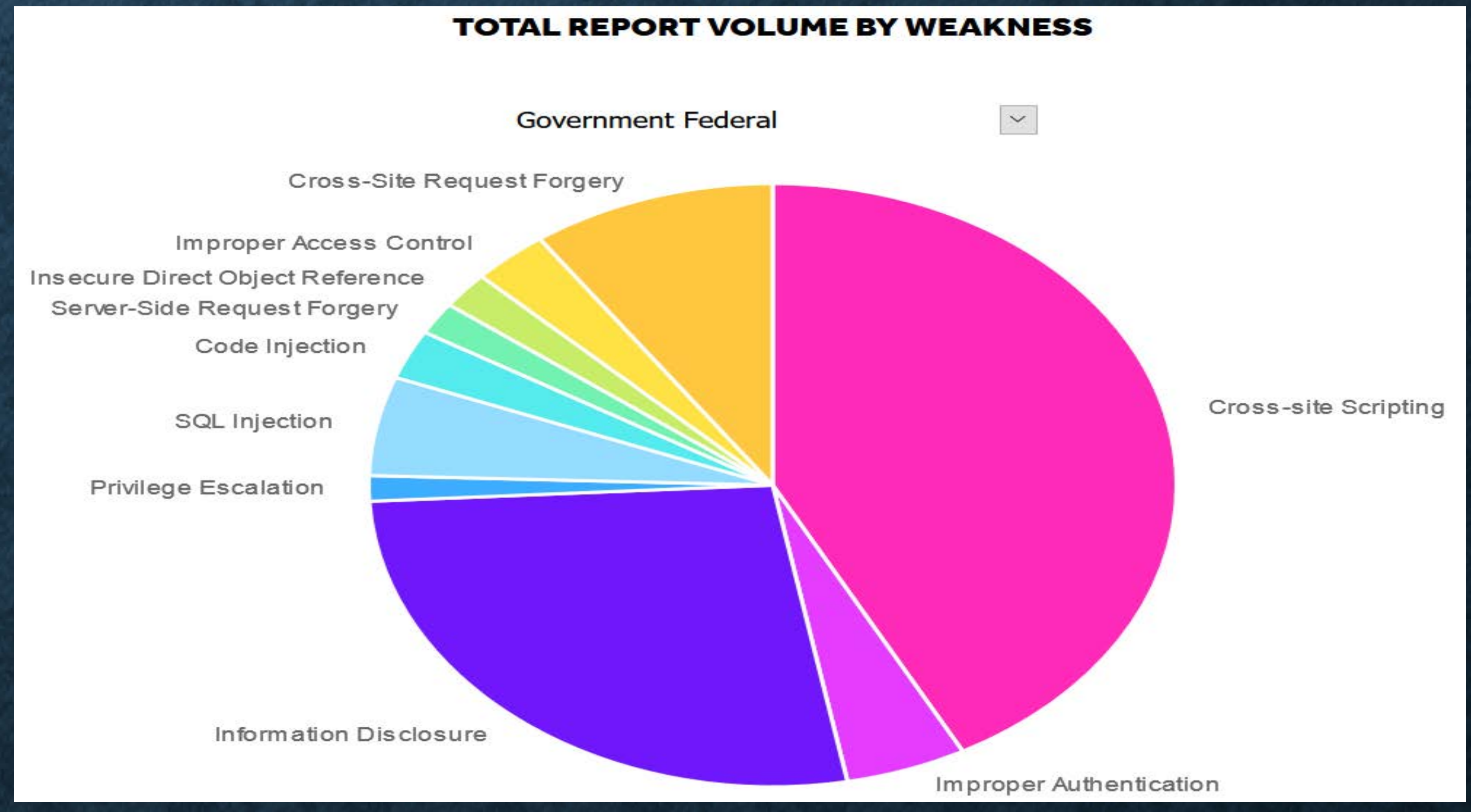
Ethical Hacker's Methodology

Results

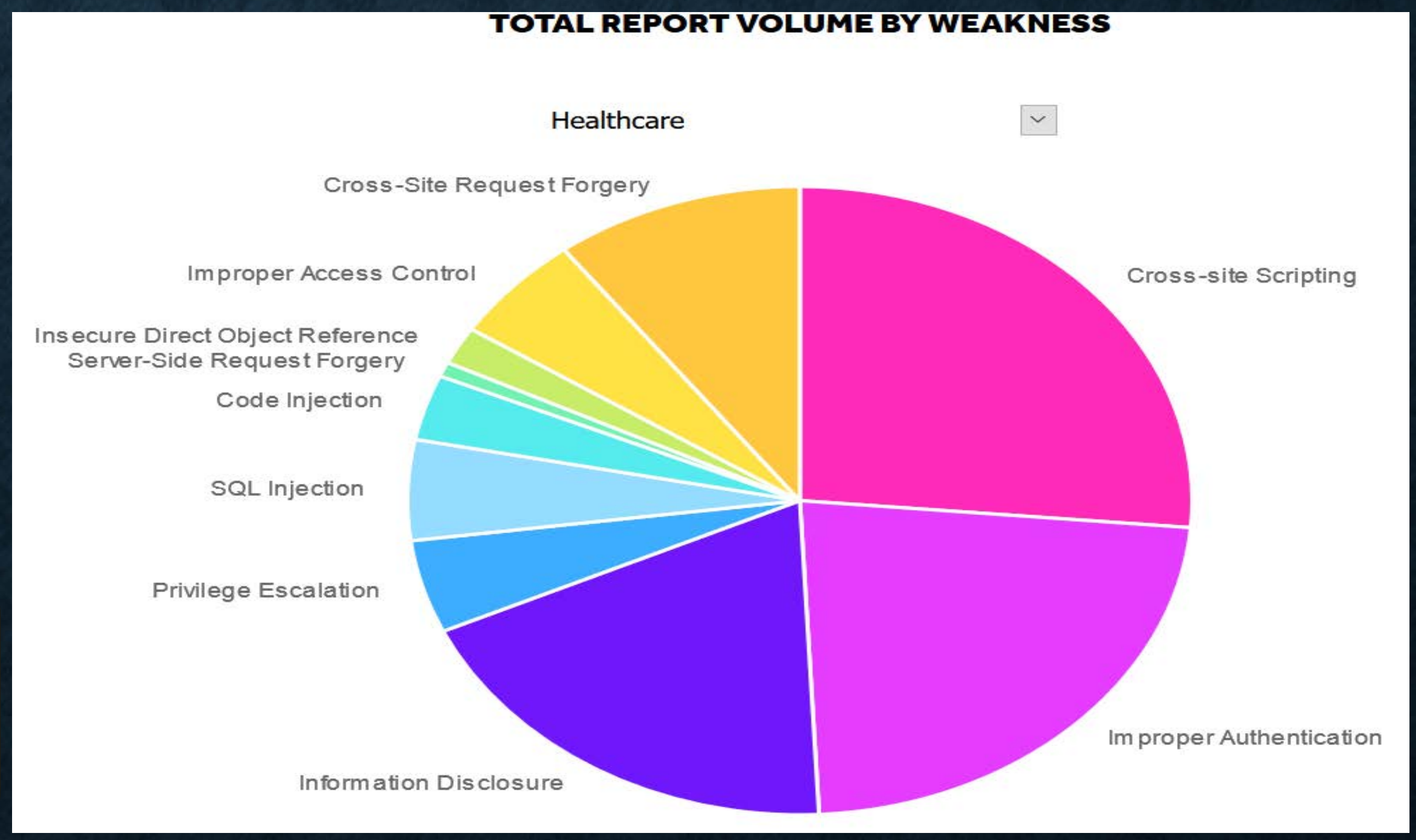


TOTAL REPORT VOLUME BY WEAKNESS

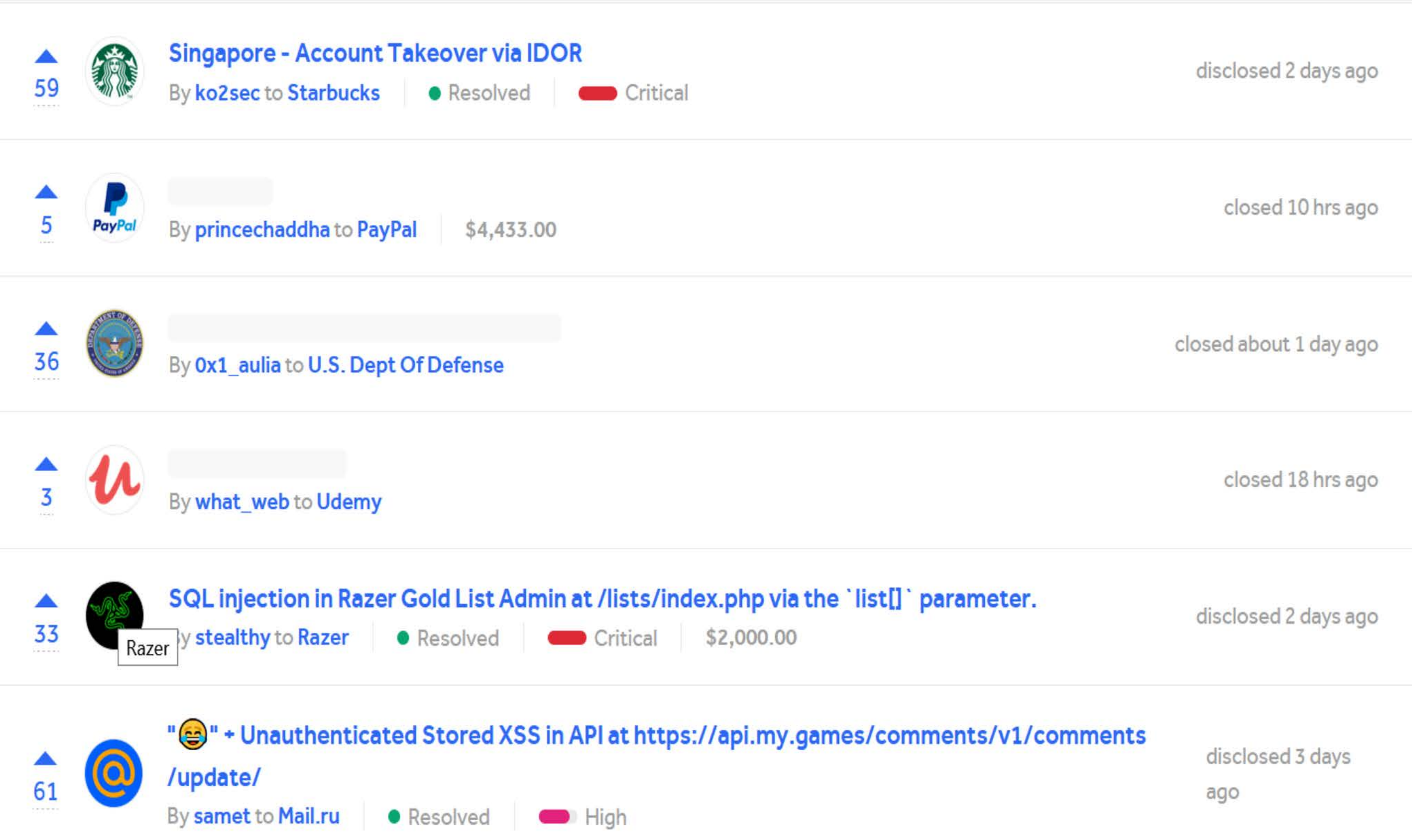
	Healthcare	Retail & eCommerce	Computer Software	Internet & Online Services
Cross-site Scripting	26%	27%	29%	30%
Improper Authentication	23%	17%	24%	18%
Information Disclosure	19%	23%	18%	23%
Privilege Escalation	5%	5%	7%	5%
SQL Injection	5%	2%	1%	3%
Code Injection	3%	2%	2%	2%
Server-Side Request Forgery	1%	1%	1%	1%
Insecure Direct Object Reference	2%	3%	2%	2%
Improper Access Control	6%	5%	4%	4%
Cross-Site Request Forgery	10%	16%	11%	12%



TOTAL REPORT VOLUME BY WEAKNESS



TOTAL REPORT VOLUME BY WEAKNESS



59 — Singapore - Account Takeover via IDOR — By ko2sec to Starbucks · Resolved · Critical — disclosed 2 days ago

5 — By princechaddha to PayPal · $4,433.00 — closed 10 hrs ago

36 — By 0x1_aulia to U.S. Dept Of Defense — closed about 1 day ago

3 — By what_web to Udemy — closed 18 hrs ago

33 — SQL injection in Razer Gold List Admin at /lists/index.php via the `list[]` parameter. — By stealthy to Razer · Resolved · Critical · $2,000.00 — disclosed 2 days ago

61 — "😂" + Unauthenticated Stored XSS in API at https://api.my.games/comments/v1/comments/update/ — By samet to Mail.ru · Resolved · High — disclosed 3 days ago

Discussion

The first documented case of "hacking" was back in the 1970's when computerized phones were becoming targeted. Since then it has shown that the more complex the system was, the more susceptible and vulnerable to cybercrime they became. In 2020, a cybersecurity firm, Trustwave, uncovered a backdoor malware named "GoldenSpy" that was embedded in mandatory Chinese tax software suites that foreign companies, doing business in China, must use to pay their taxes. By way of social engineering, Twitter had a major breach in their systems and hackers were able to swindle numerous individuals of roughly $120,000 in BitCoin. Cybercriminals posed as Amazon employees to steal money and personal information from unsuspecting customers. These two examples were accomplished not by attacking the system, but rather by exploiting one of the only open-ended variables in the equation, the human factor.

Some reactive and defensive methods of security protocols are virus scanners (Norton, Avira, McAfee), software updates that include bug fixes, malware detection, and firewalls. The Catch-22 behind this approach is the need for existence of a threat before you can detect and disable it. Ethical hacking and penetration testing are two of the proactive approaches to prevent security breaches before they arise. Essentially, these tactics are innocuously executed to find flaws and patch them before they can be exploited for nefarious purposes. Some companies openly invite, challenge and reward people to successfully hack their systems known as the "Bug Bounty" program. Sony offered $50,000 to anyone who could hack Playstation4. While defenders have to find all the bugs in a system, attacker need only to find one flaw to infiltrate the system.

Advantage

- Helping in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevent website defacements
- Fight against terrorism and national security breaches
- Having a computer system that prevents malicious hackers from gaining access

Disadvantage

- All depends upon the trustworthiness of the ethical hacker
- Hiring professionals is expensive
- The ethical hacker using the knowledge they gain to do malicious hacking activities
- Allowing the company's financial and banking details to
- be seen Massive security breach

Conclusions

- ❑ Cyber crime is predicted to increase exponentially.
- ❑ A proactive approach to cyber security is needed and reactive security measures are not enough. Ethical hacking fills that void.
- ❑ Ethical Hacking is proven to prevent cyber crime and security breaches on computer networks and systems.

Acknowledgements

I want to thank STEM SSA Director Dr. Reena Randhir and DHE for the encouragement and support. I also want to thank all the staff and guest speakers that shared their time and expertise.