AVOIDING THE OWASP

Top 10 security exploits

ME

- Certified Penetration Testing Engineer
- Certified Ethical Hacker
- Master’s in Information Technology (CyberSec)

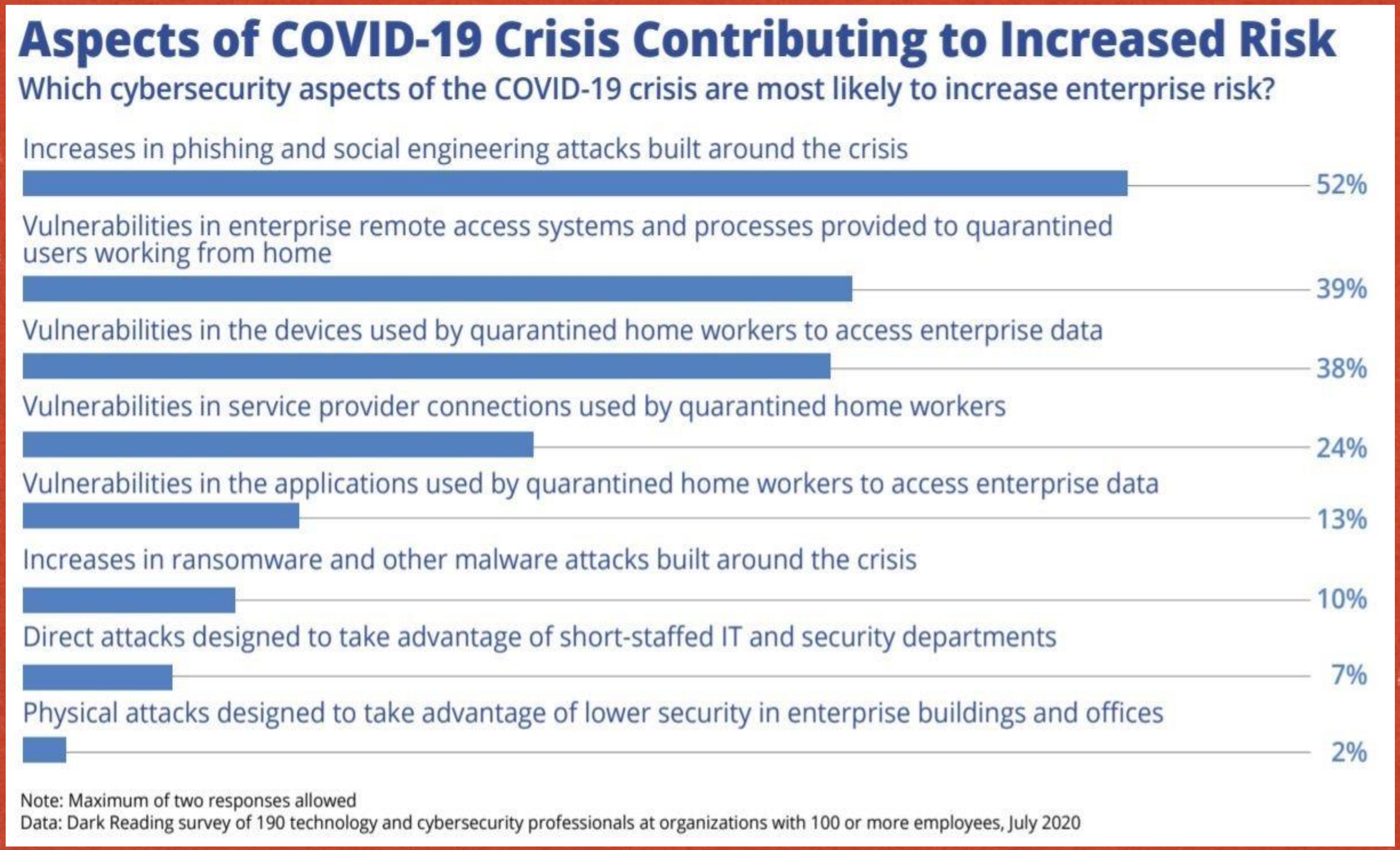

SECURITY

SECURITY CONTINUUM

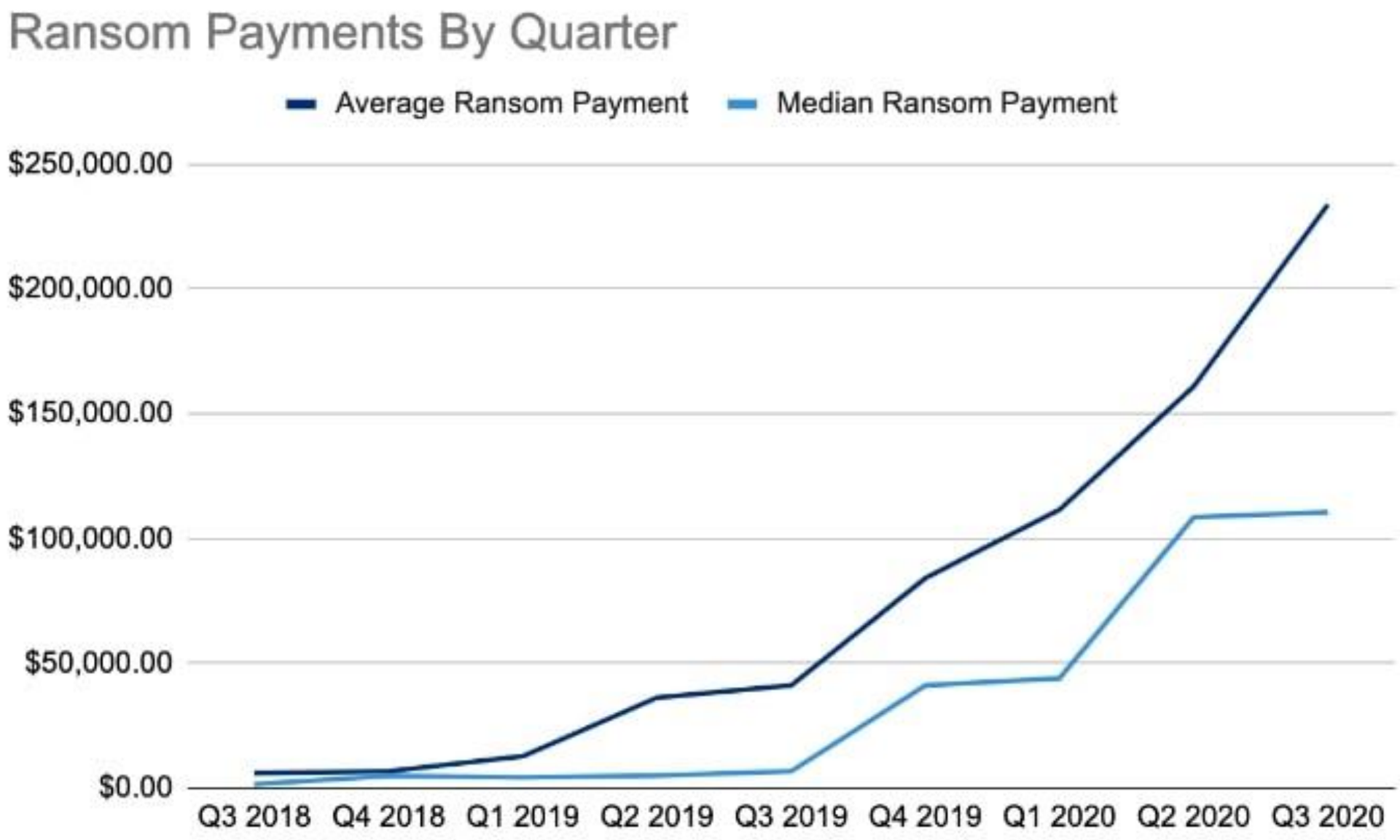
unusable

unrestricted

Some Statistics on Security



Some Statistics on Security



COVEWARE

Some Statistics on Security

Top 10 most valuable information to cyber criminals	Top 10 biggest cyber threats to organizations
1. Customer information (17%)	1. Phishing (22%)
2. Financial information (12%)	2. Malware (20%)
3. Strategic plans (12%)	3. Cyberattacks (to disrupt) (13%)
4. Board member information (11%)	4. Cyberattacks (to steal money) (12%)
5. Customer passwords (11%)	5. Fraud (10%)
6. R&D information (9%)	6. Cyberattacks (to steal IP) (8%)
7. M&A information (8%)	7. Spam (6%)
8. Intellectual property (6%)	8. Internal attacks (5%)
9. Non-patented IP (5%)	9. Natural disasters (2%)
10. Supplier information (5%)	10. Espionage (2%)

OWASP

Open Web Application Security Project

- Worldwide non-profit organization aimed to improve security.
- Reaches out to all developers, IT personnel and individuals, not just security professionals.
- All material is free and easily accessible.


OWASP TOP 10

INJECTION

```
' OR 1=1 '--
```

RISKS

- Permits query manipulation and arbitrary SQL.
- Command - Permits use of shell commands.
- Attackers can run code/queries for unauthorized access.

SQL INJECTION EXAMPLE

SQL Injection Example

User-Id: sanil

Password: newpwd

```
select * from Users where user_id = ' sanil ' and password =
' newpwd '
```

User-Id: ' OR 1 = 1; /*

Password: */ --

```
select * from Users where user_id = '' OR 1 = 1; /* ' and
password = ' */ -- '
```

PREVENTION

- "Connections" between systems are highly vulnerable
- Always assume data coming in could be "evil“ be sure to include "evil" use cases and user stories in your design
- Sanitize and Validate user submitted data.
- If user-input text is needed, use parameterized queries clean up quotes, parenthesis, and SQL comments

BROKEN AUTHENTICATION & SESSION MANAGEMENT

/index.php?PHPSESSID=pwned

RISKS

- Identity theft.
- Access to unauthorized and sensitive data.
- Attackers can steal a cookie for session hijacking.
- Possible brute force attack utilizing data breaches.

SESSION & COOKIES

- Http is a “stateless” protocol.
- Store the state with session (server) and cookies (client).
- Session IDs are stored in cookies or url.
- Packet Sniffing, HttpReferrer Logs, etc.

PREVENTION

- Implement **updated** SSL/TLS everywhere.
- Have cryptographically strong session ID.
- Use two-factor authentication wherever possible.
- Use rate limiting for repeated login attempts.

XSS

```
<script>alert('cross site scripting');</script>
```

RISKS

- Can be used to run malicious scripts on website.
- Can lead to multiple kinds of attack.
- Used to steal session cookies.
- Combined with phishing, it can be used to steal sensitive data .

XSS EXAMPLE

Cross-Site Scripting Illustrated

1 Attacker sets the trap – update my profile

Application with stored XSS vulnerability

2 Victim views page – sees attacker profile

3 Script silently sends attacker Victim's session cookie

OWASP - 2010

PREVENTION

- Never, ever, ever trust user submitted data (e.g. URLs, web forms, comment threads, etc.)
- Implement content security policy.
- Set HttpOnly flag.
- Convert special characters such as ?, &, /, <, > and spaces to their respective HTML or URL encoded equivalents.

Q & A

THANK YOU!