CYBER ATTACK – RANSOMWARE and other Fruits…

Presenter: Oren Elimelech, Ministry of Transport Israel Cyber Adviser (ISACA Israel Chapter)
CyberTeam360 CEO & Founder
CISO, CISM, CRISC, CISA, CISSP, EnCE, PCIP, DFR

19 October 2020

CYBERTEAM 360
protecting what matters

WEBINAR REMINDER

- You’re more than welcome to send your questions during the Webinar, but they will be answered at the Q&A session after the presentation.

WHAT IS A RANSOM?

- Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it

- Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert

- There are targeted attacks and there are un-targeted attack (spray)

Who am I ?

- Age 45 – Computer & IDF Electronics Practical Engineer
- Israel Ministry of Transport and Road Safety Cyber Security Adviser
- Cyber Security & Privacy Researcher, Expert & Adviser
- CISM ISACA Israel chapter trainer + many other certifications…
- Research Associate @ International Institute for Counter-Terrorism ICT
- Founder of CyberTeam360
  - Cybersecurity solutions boutique firm and research hub, providing high-end specialized security governance, assessments, training and consulting services for the private and government sectors

CYBERTEAM360
protecting what matters

RANSOMWARE 2020

The Growing Cost
The Global Cost of Ransomware 1
Cost in Billions
$20B
$15B
$10B
$5B
$0
USD11.5 Billion
USD20 Billion
2019
2020
Average Cost by Type of Attack 2
Cost in Millions
$4M
$3M
$2M
$1M
$0
USD3.86 Million
USD4.27 Million
USD4.44 Million
Data Breach
Malicious Breach
Ransomware Attack

RANSOMWARE 2020

- Ransomware is quickly growing in scope and impact. Opinions on the subject are abundant but:
- what are the key facts?
- What is the true cost and frequency of Ransomware attacks?
- And most importantly how prepared are we to find them and contain them?

RANSOMWARE STATISTICS

Every

11 Seconds

A business is attacked by ransomware

36%

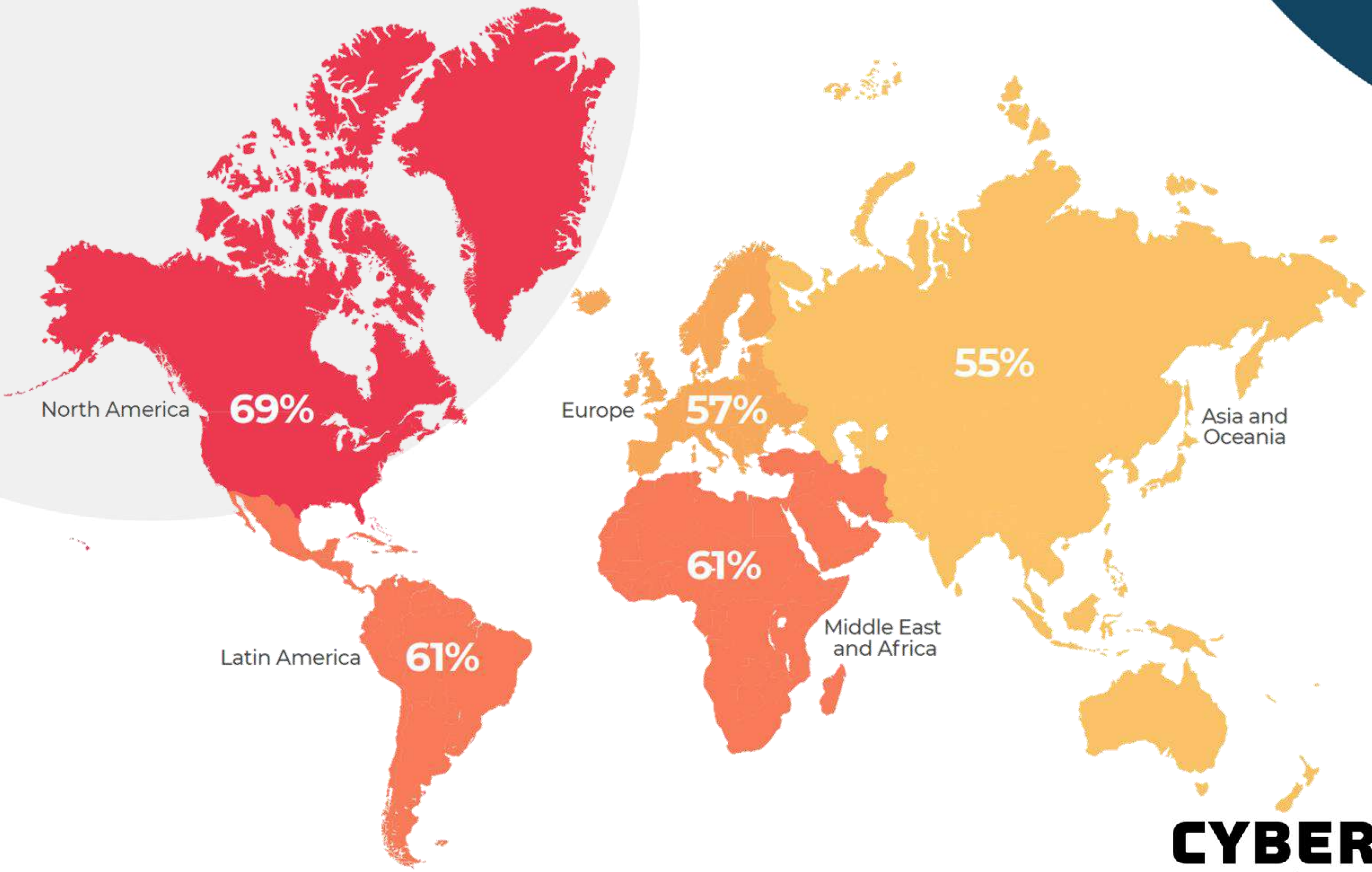
Of victims paid the ransom

17%

Of victims who paid a ransom never recovered their data

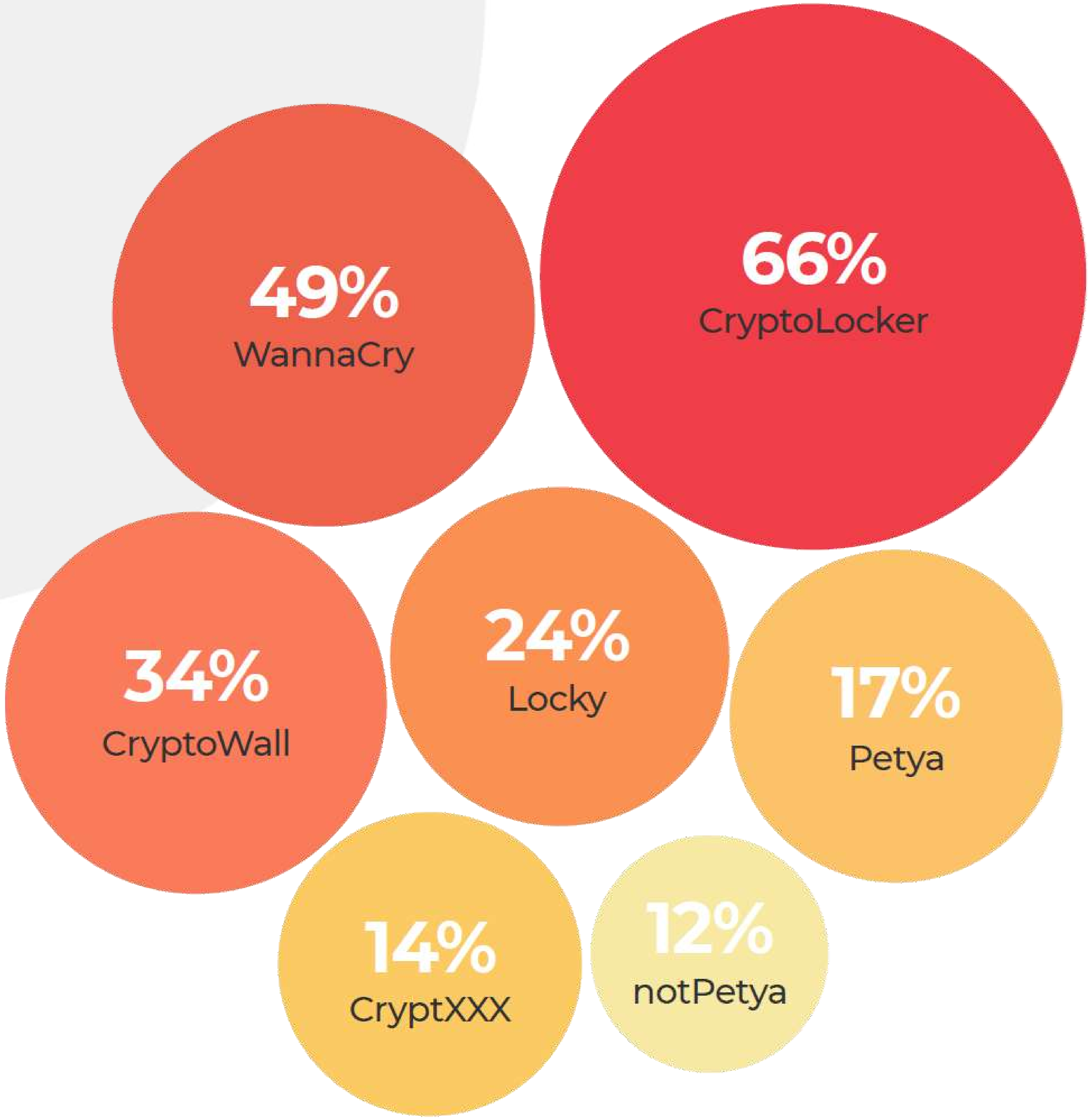
CYBERTEAM 360
protecting what matters

PERCENTAGE OF COMPANIES WHO REPORTED BEING AFFECTED BY RANSOMWARE



CYBERTEAM 360
protecting what matters

% OF NA MSPs THAT REPORTED THESE TYPE OF RANSOMWARE INCIDENTS



CYBERTEAM 360
protecting what matters

INDUSTRIES REPORTING RANSOM ATTACKS IN THE LAST YEAR

Government	15.4%
Manufacturing	13.9%
Construction	13.2%
Utilities	11.1%
Services	10.4%
Retail	7.5%
Real Estate	7.1%
Hospitality	6.1%
Healthcare	5.7%
Education	5%
Financial	4.6%

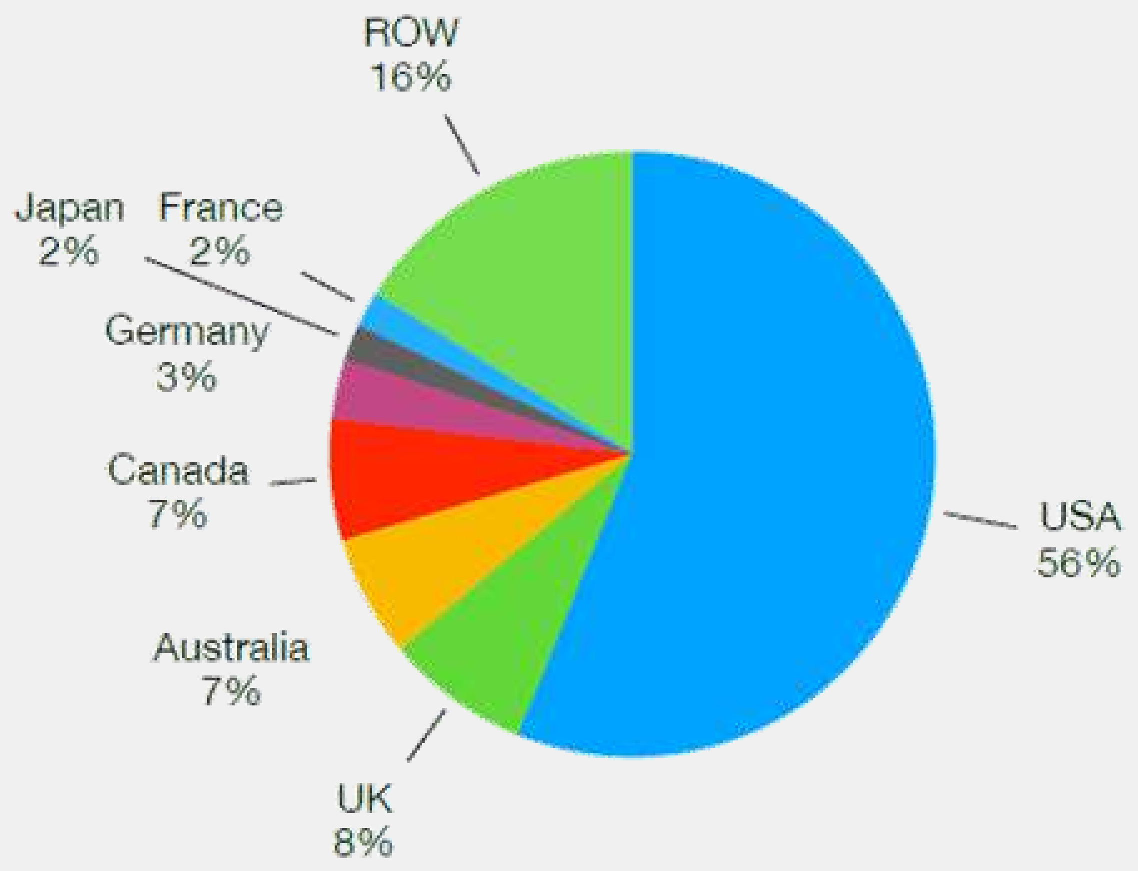
INDUSTRIES REPORTING RANSOM ATTACKS IN THE LAST YEAR

28% of SMBs said they do not have a plan to mitigate a ransomwate attack

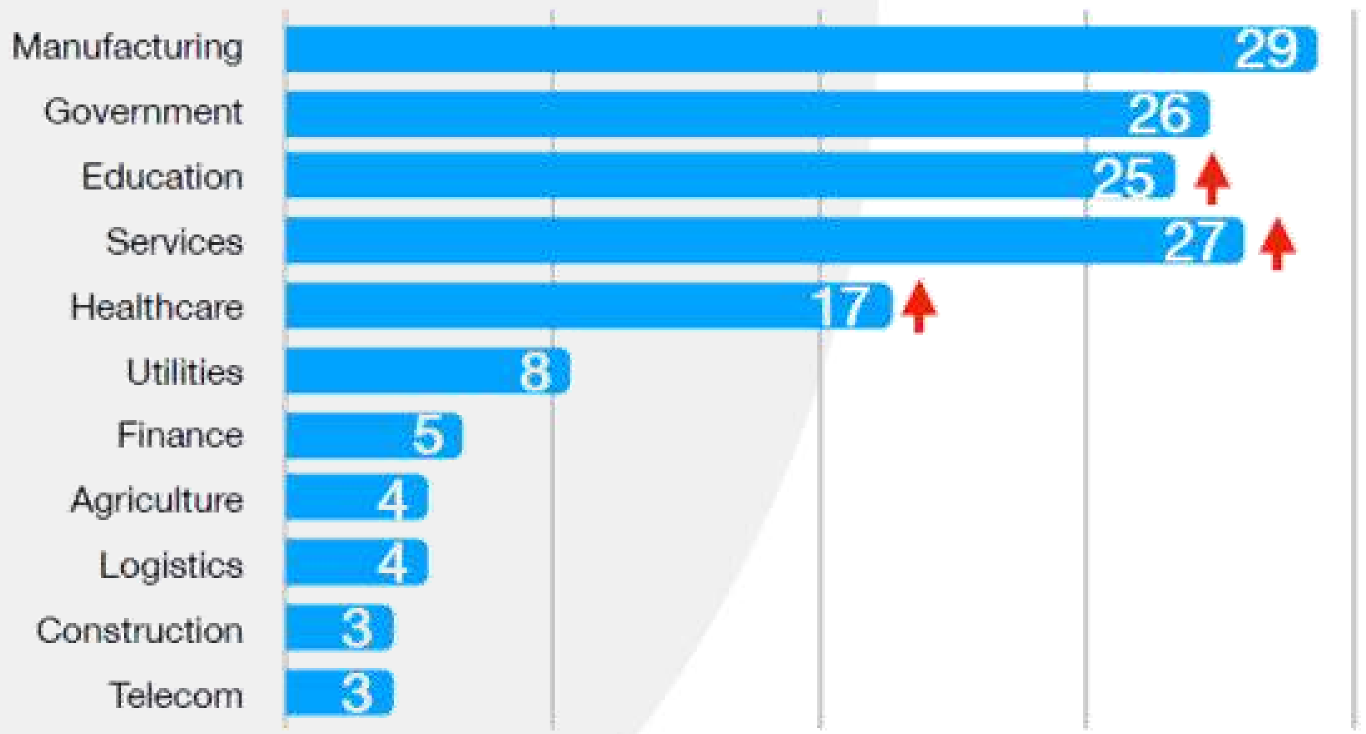
CYBERTEAM 360
protecting what matters

GLOBAL RANSOMWARE – JAN – SEP 2020

Attacks by Country



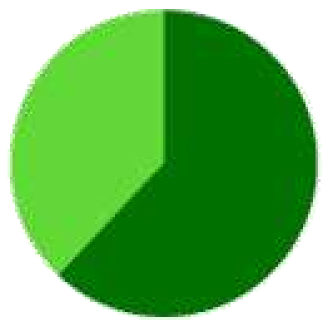
Attacks by Industry



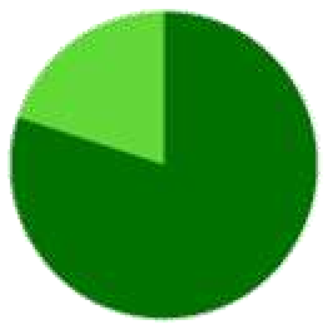
Key Trends

Average ransomware payment

US$178,254 +60%

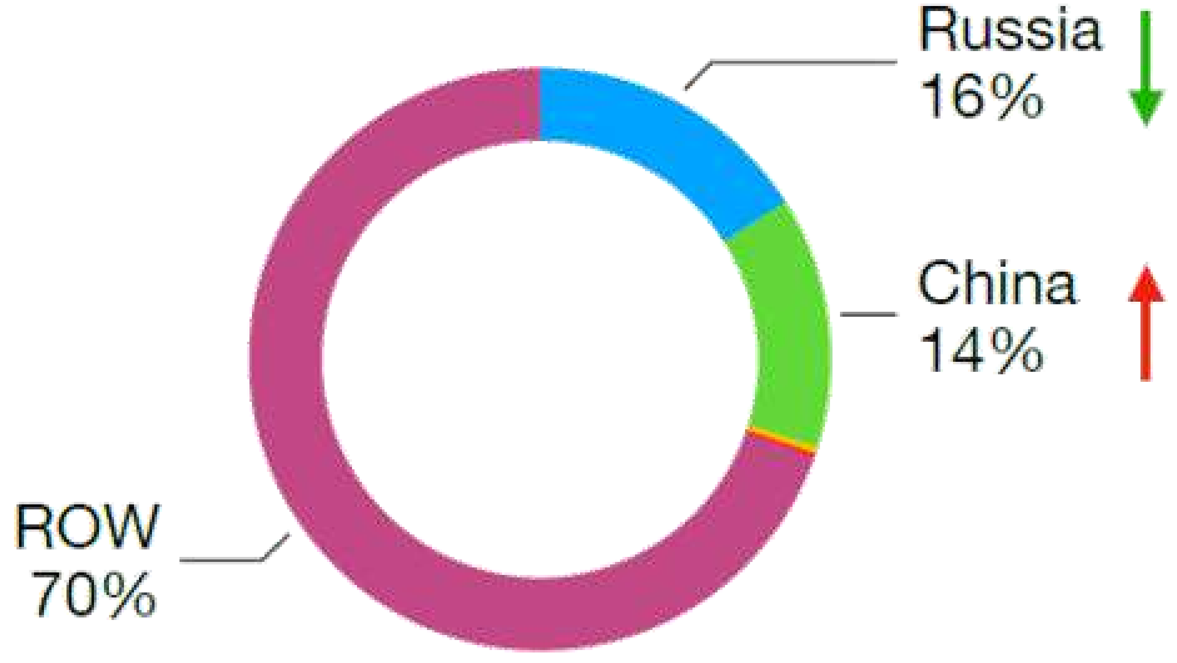


62% of all attacks Ransomware

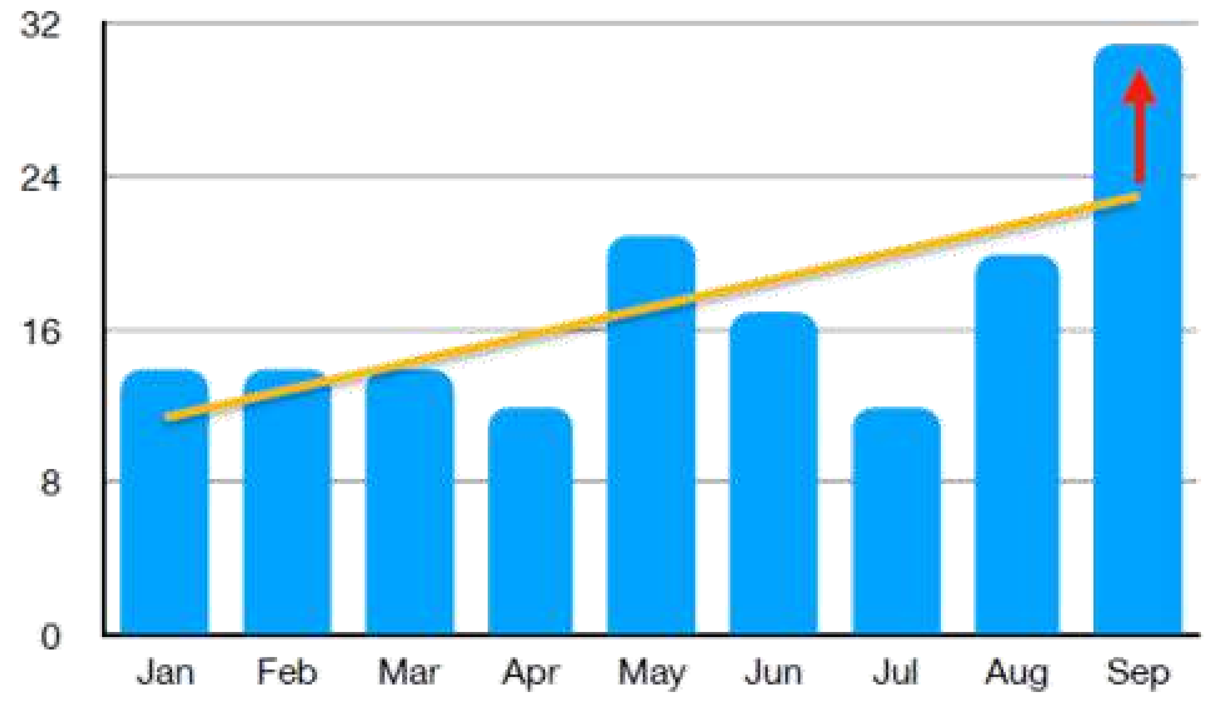


80% of attacks exfiltrate data

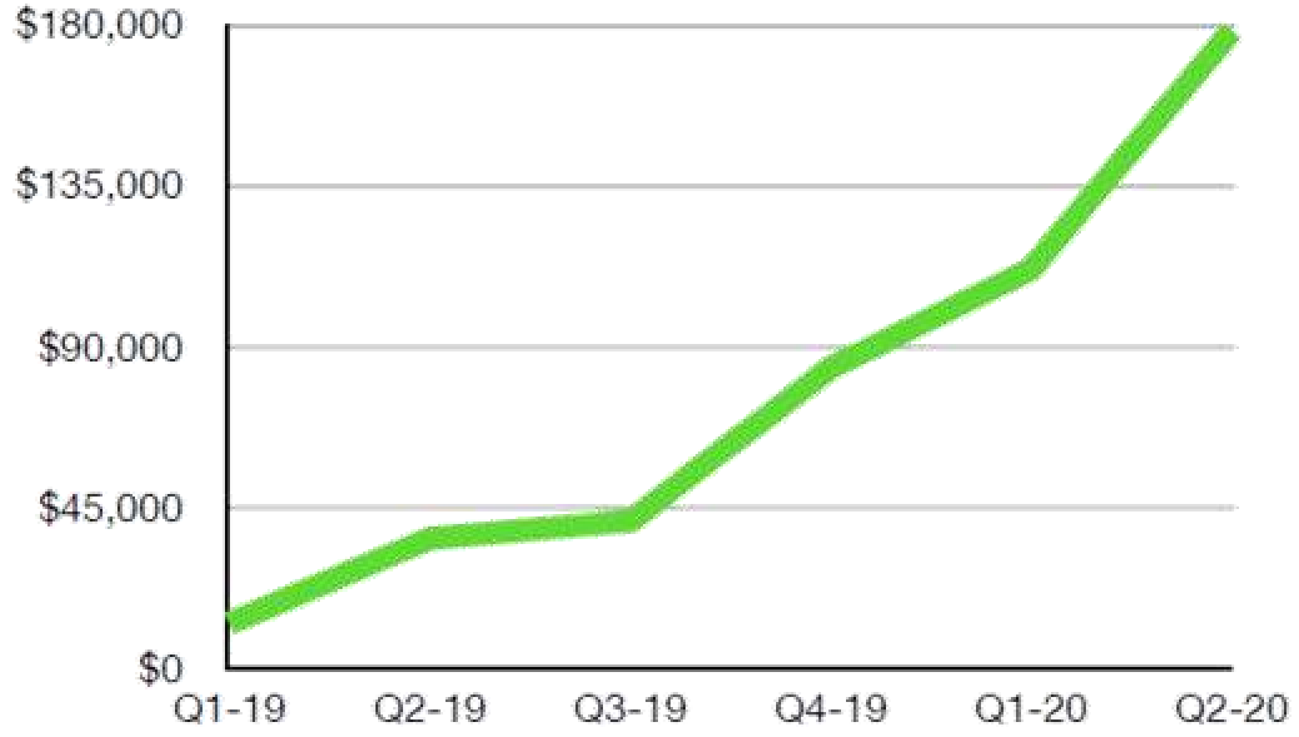
Ransomware Exfiltration



Attack Trend by Month



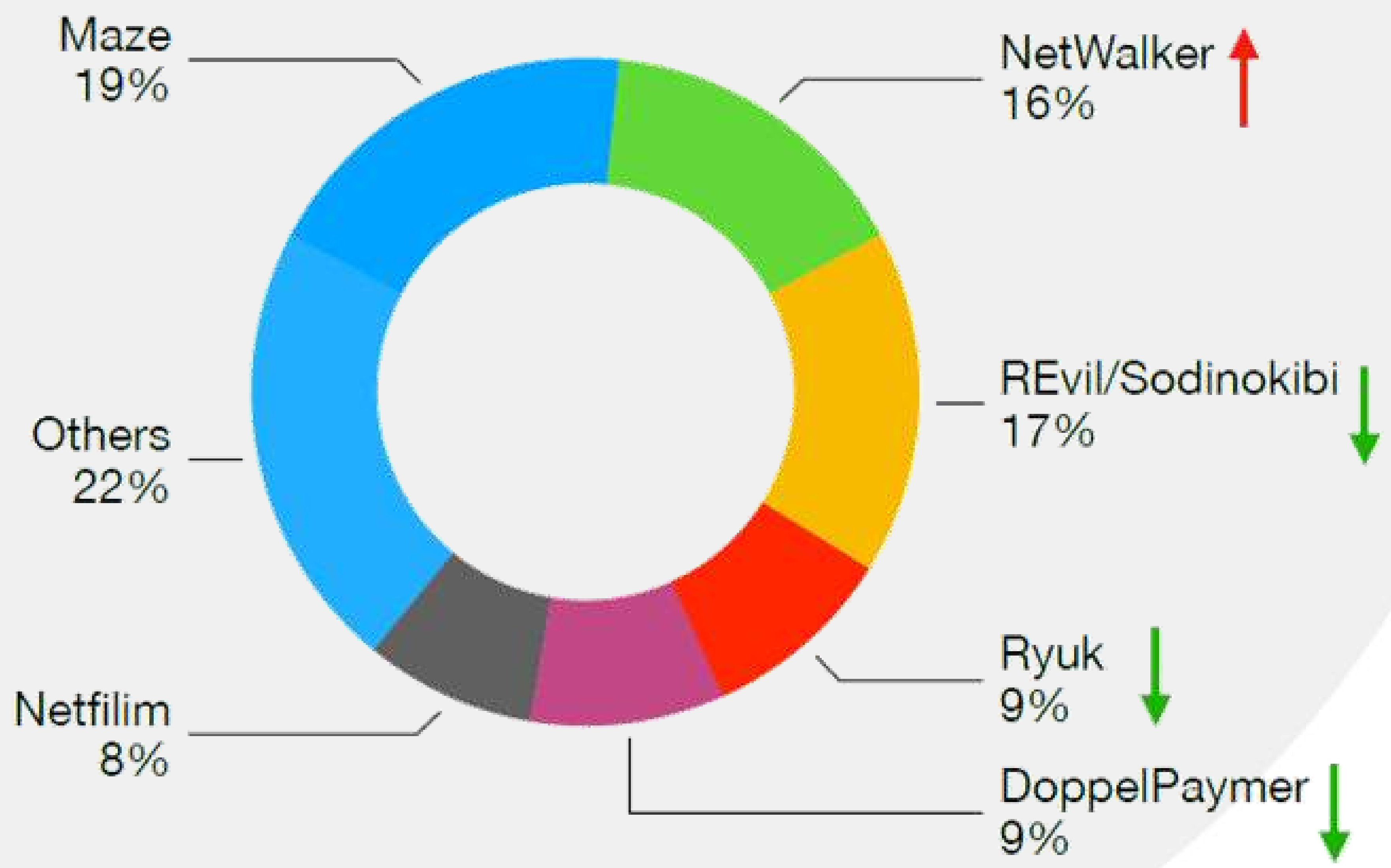
Average Ransom Payout[1]



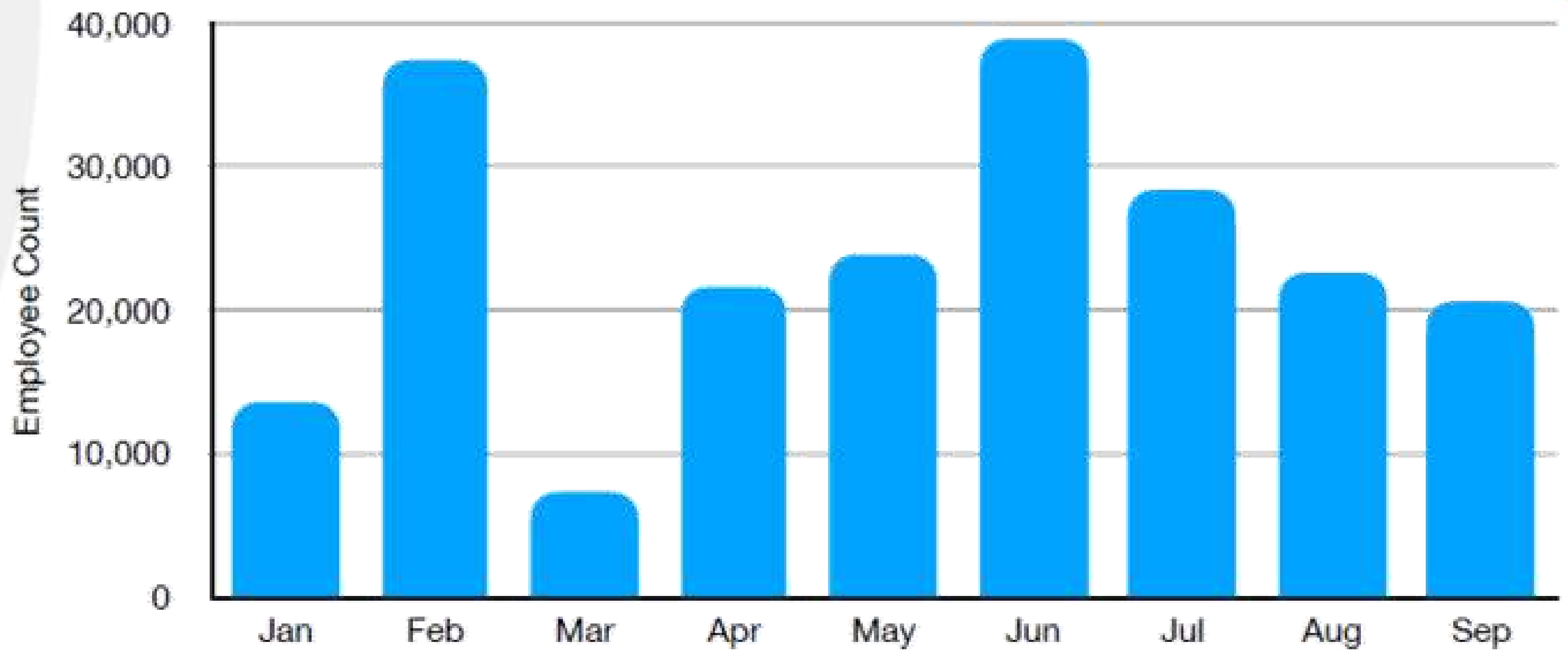
CYBERTEAM 360
protecting what matters

GLOBAL RANSOMWARE – JAN – SEP 2020

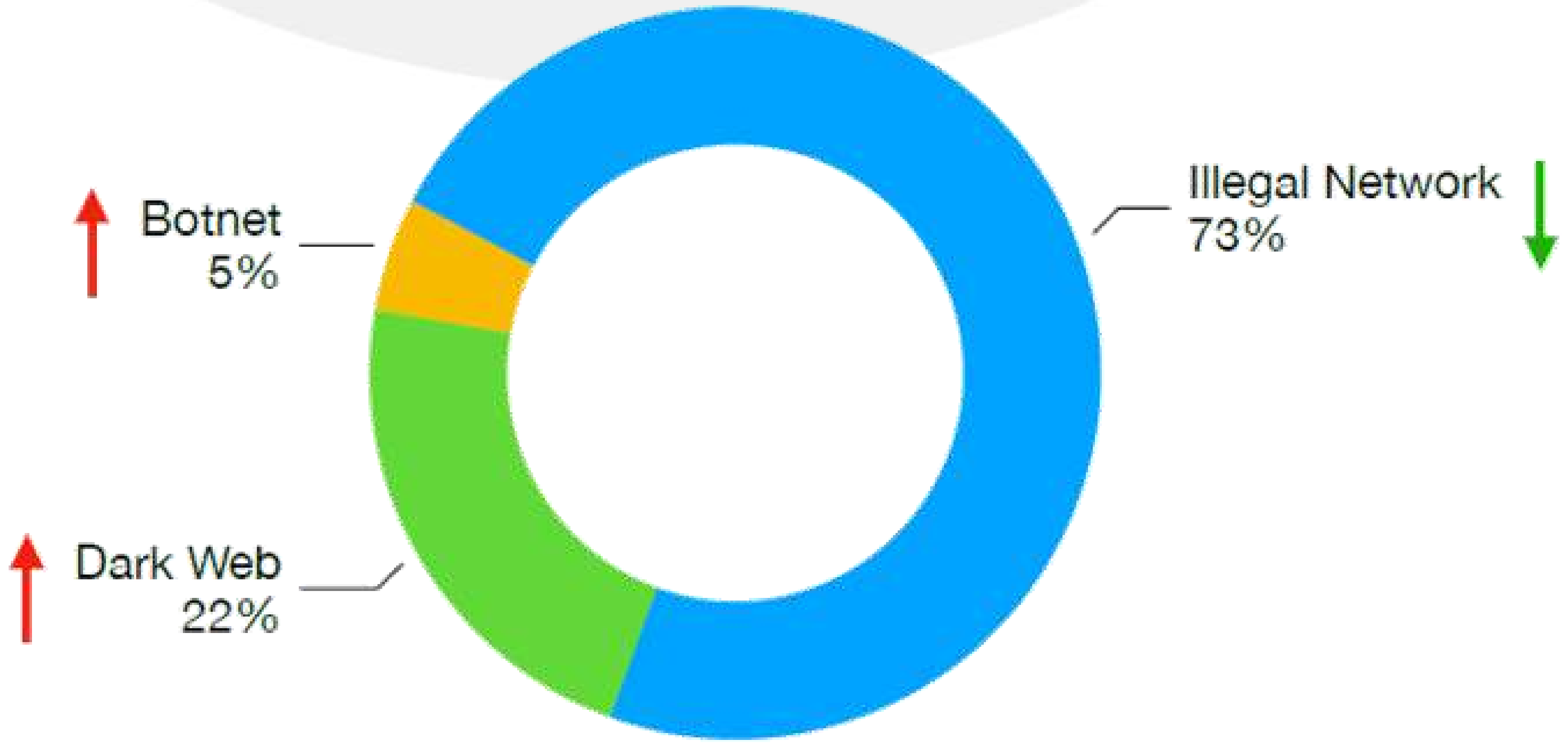
Threats by Variant



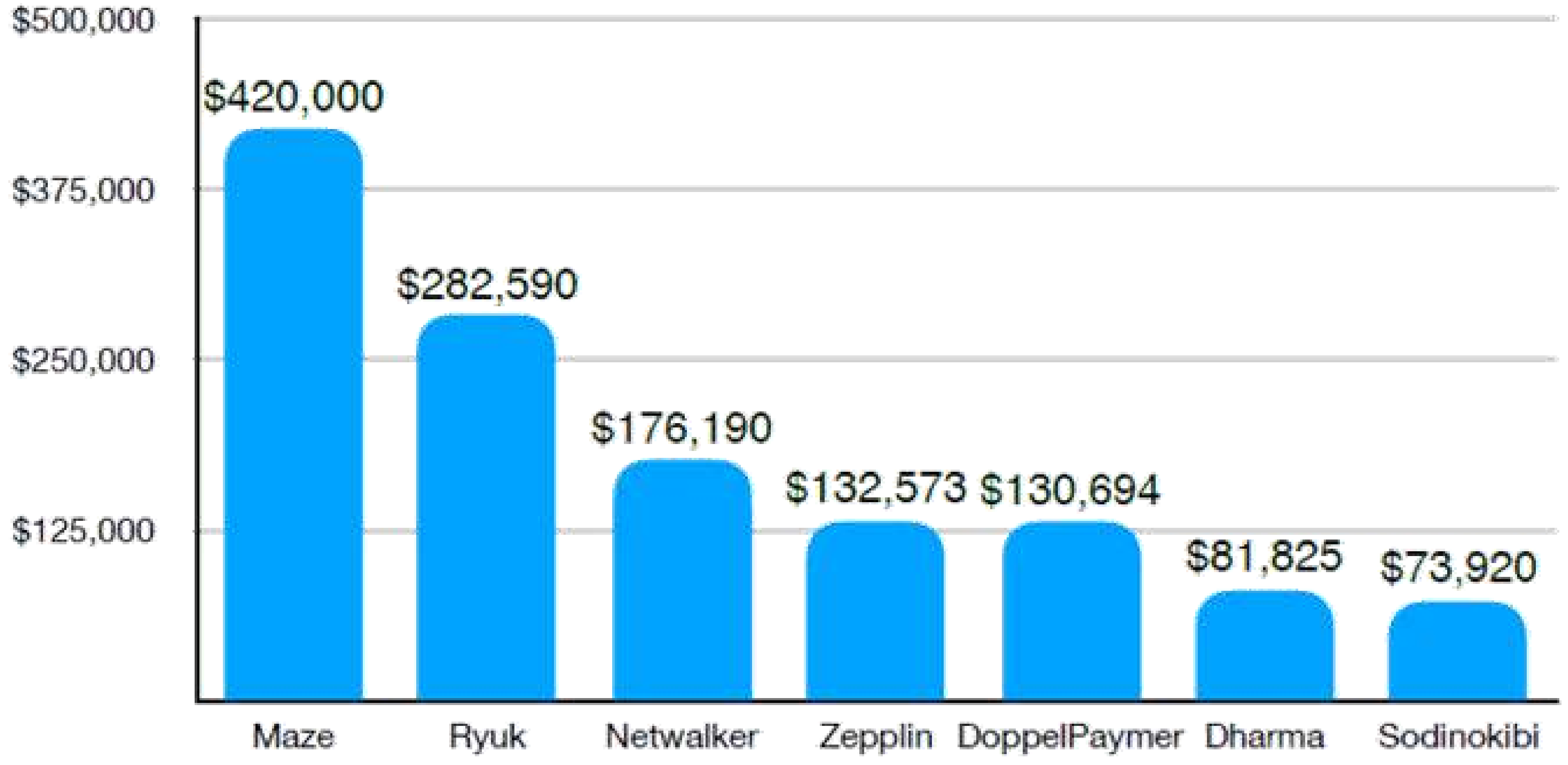
Average Size of Organization



Ransomware Exfiltration Techniques



Average ransom demand by strain[2]



CYBERTEAM 360
protecting what matters

PREPARDNESS AND PREVENTION

Gartner analysis of clients’ ransomware preparedness shows that over **90% of ransomware** attacks are preventable

REFERENCE SOURCES

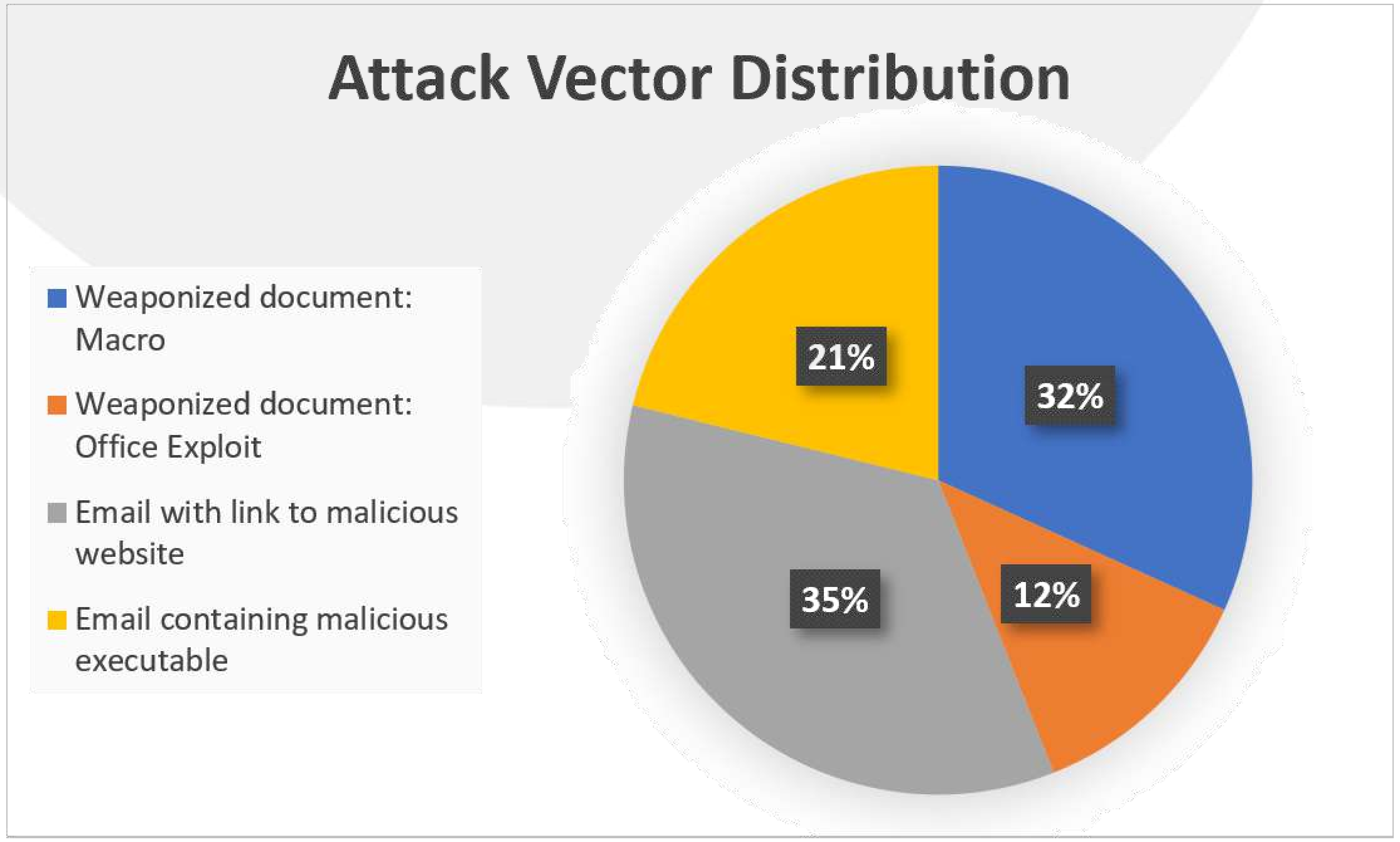
- Cybersecurity Ventures - Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
- 2020 IBM Cost of a Data Breach report
- Kaspersky Story of the Year: The Ransomware Revolution
- CyberEdge 2020 CDR Report
- CCIT: Informe de las Tendencias del Cibercrimen en Colombia (2019-2020)
- Safety Detectives: Ransomware Facts, Trends & Statistics for 2020
- Infrascale Ransomware Survey
- Gartner: Defend Against and Respond to Ransomware Attacks, 2019
- Coalition: Report
- Coveware: First responders report

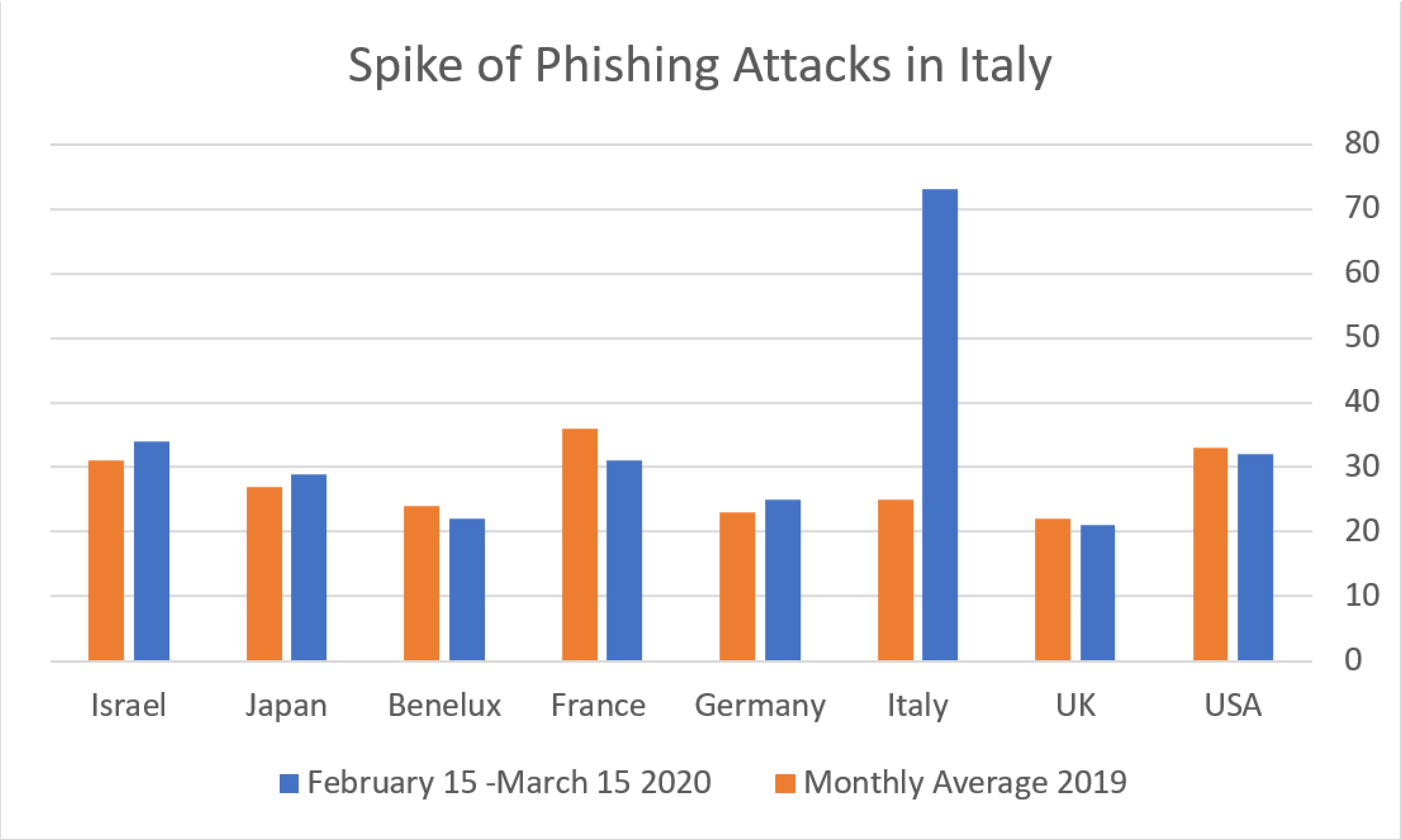
Remote work and Cybersecurity: Coronavirus threats

Why is Cybersecurity so important during COVID-19?

SOME STATISTICS

- During COVID-19-related phishing attacks up by 667%





CYBERTEAM 360
protecting what matters

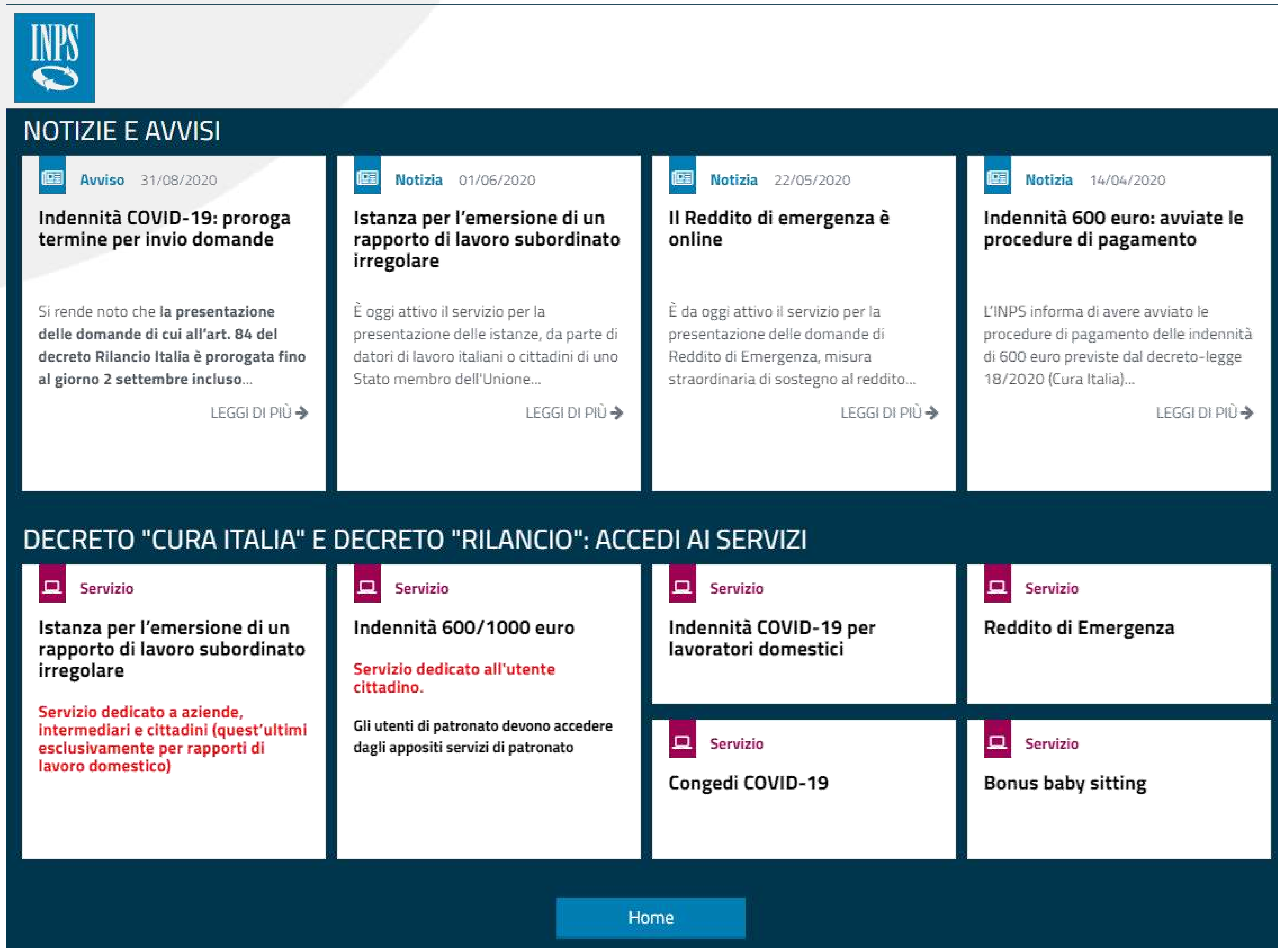
SOME STATISTICS ON COVID-19 ERA

- 22% of breaches involve phishing
- 96% of phishing attacks arrive by email
- Top 5 Data “types” that are compromised by breaches:
  - **Credentials** (passwords, usernames, pin numbers)
  - **Personal data** (name, address, email address)
  - **Internal data** (sales projections, product roadmaps)
  - **Medical** (treatment information, insurance claims)
  - **Bank** (account numbers, credit card information)
- 95% of attacks are motivated by intelligence gathering
- Targeted attacks - 65% of active groups relied on spear-phishing as the primary infection vector
  - This is followed by watering hole websites (23%), trojanized software updates (5%), web server exploits (2%), and data storage devices (1%)

ON APRIL 2020

- Italian Social Service Website Is Subject To A Cyber-Attack!

- INPS's website in Italy was attacked as about 339,000 applications for the €600 benefits for VAT-registered and self-employed Italians were being processed



INPS

NOTIZIE E AVVISI

Avviso 31/08/2020

Indennità COVID-19: proroga termine per invio domande

Si rende noto che **la presentazione delle domande di cui all'art. 84 del decreto Rilancio Italia è prorogata fino al giorno 2 settembre incluso**...

LEGGI DI PIÙ →

Notizia 01/06/2020

Istanza per l'emersione di un rapporto di lavoro subordinato irregolare

È oggi attivo il servizio per la presentazione delle istanze, da parte di datori di lavoro italiani o cittadini di uno Stato membro dell'Unione...

LEGGI DI PIÙ →

Notizia 22/05/2020

Il Reddito di emergenza è online

È da oggi attivo il servizio per la presentazione delle domande di Reddito di Emergenza, misura straordinaria di sostegno al reddito...

LEGGI DI PIÙ →

Notizia 14/04/2020

Indennità 600 euro: avviate le procedure di pagamento

L'INPS informa di avere avviato le procedure di pagamento delle indennità di 600 euro previste dal decreto-legge 18/2020 (Cura Italia)...

LEGGI DI PIÙ →

DECRETO "CURA ITALIA" E DECRETO "RILANCIO": ACCEDI AI SERVIZI

Servizio

Istanza per l'emersione di un rapporto di lavoro subordinato irregolare

Servizio dedicato a aziende, intermediari e cittadini (quest'ultimi esclusivamente per rapporti di lavoro domestico)

Servizio

Indennità 600/1000 euro

Servizio dedicato all'utente cittadino.

Gli utenti di patronato devono accedere dagli appositi servizi di patronato

Servizio

Indennità COVID-19 per lavoratori domestici

Servizio

Reddito di Emergenza

Servizio

Congedi COVID-19

Servizio

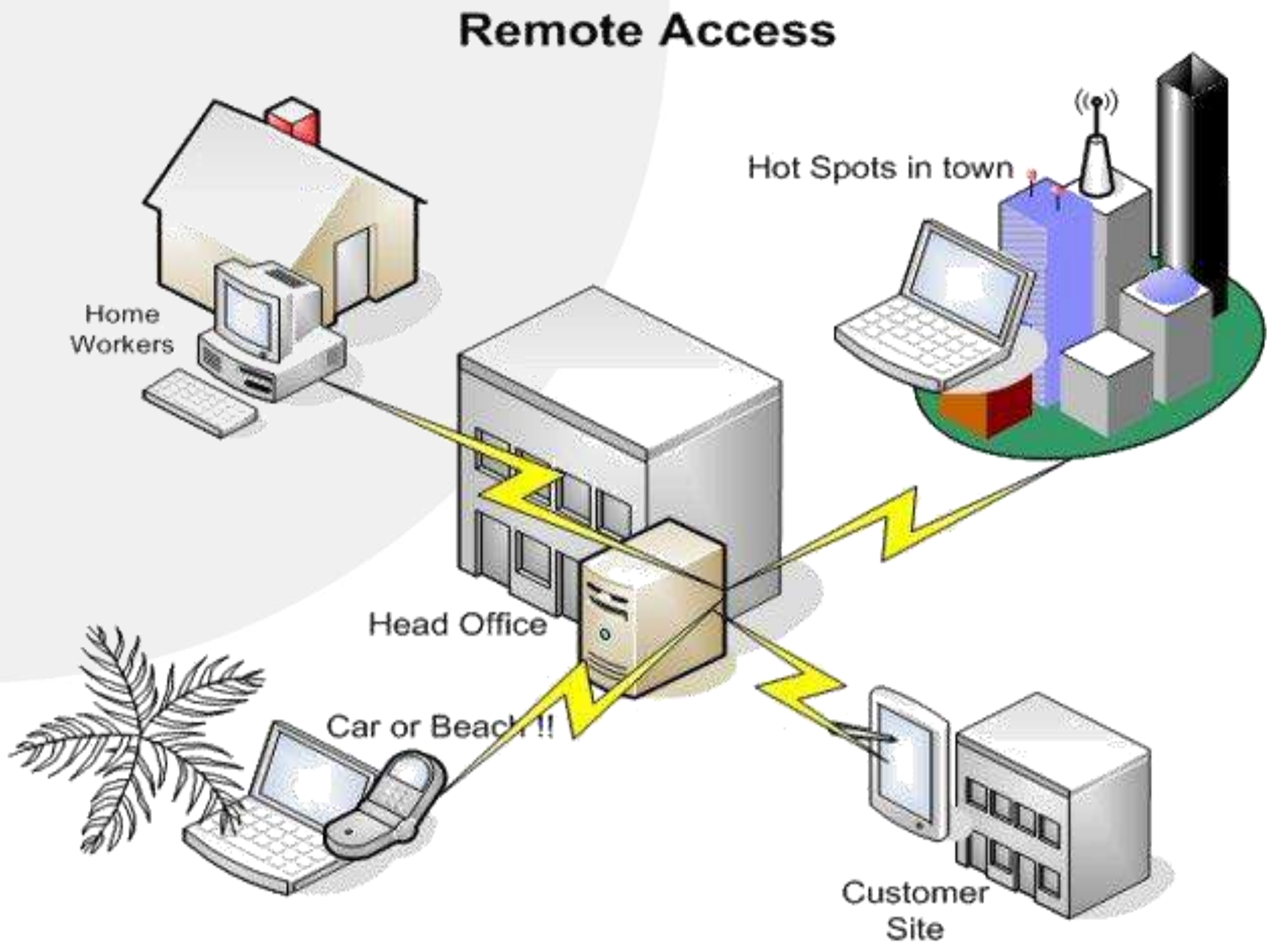
Bonus baby sitting

HOW COVID-19 HAS CHANGED OUR DAILY ROUTINE

- Following the effects of Covid-19, companies are accelerating the transition to remote work. While necessary from a health and business continuity perspective, this trajectory introduces additional cyber threats to an already challenging environment.

- Cyber adversaries have been quick to take advantage of the situation. Attackers leverage the expanding attack surface, exploit technical vulnerabilities intrinsic to remote connectivity, home environments and cloud, and implement new forms of social engineering attacks.
  - Be sure to lock your computer immediately when you step away
  - Social Engineers attacks - High profile news items are often exploited by hackers
  - Open Coronavirus emails with great caution

REMOTE ACCESS DIAGRAM



SECURITY TEAMS CHALLENGE

- The transition of working from home is causing changes, not just network wise by connecting to assets remotely but also in processes that are not necessary enforced in the way that they should be.

- Since the network access and behavior patterns changed (for instance increase use of VPN access) the past learned baselines (current-old status) and the thresholds are no longer valid. This leads to a new problem that the old network traffic & behavior are not reflecting the new situation - leading to flooding the SOC and security teams with “false positive” security alerts. This result is due to the rapid change in employee behavioral patterns, making it harder to distinguish between genuine threats and “noise”.

HOW WE CAN REDUCE THE RISKS?

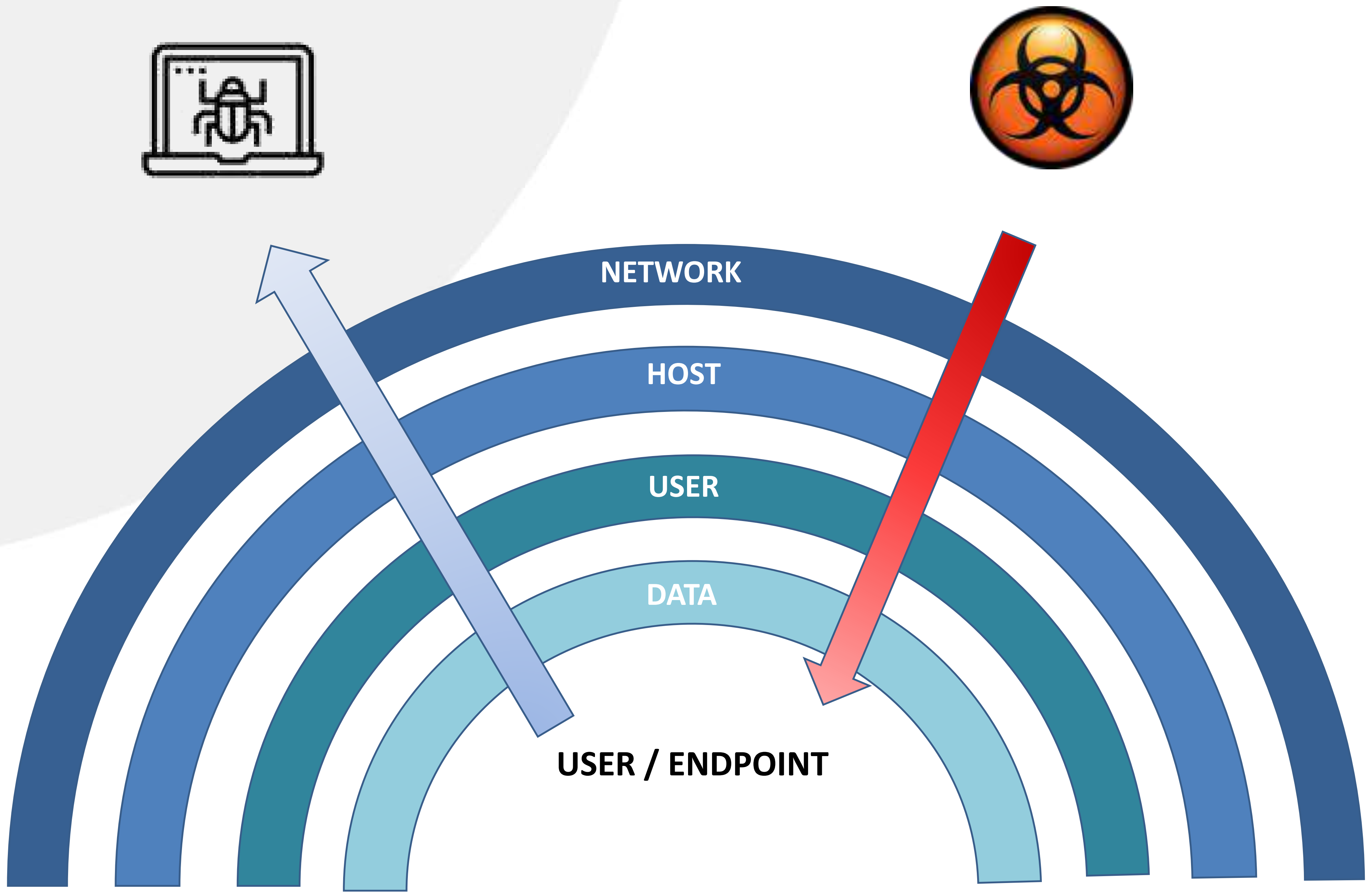
By leveraging a proactive approach to these challenges and a concentrated effort to adapt existing technologies and processes to the new threat landscape can significantly reduce the risk.

We recommend considering several security measures:

- Ensure policies are adapted to the new work environment. If process discipline was loosened, as is inevitable in many crisis management situations, make sure it's gradually restored to strong security level.
- Raise employee awareness to the new wave of social engineering attacks and fraud attempts, preying on confusion and fear (due to Covid-19 pandemic panic).
- Increase logging and visibility of remote access activities to optimize detection of adversarial events.
- Ensure and implement strong security controls and counter-measures to all existing cloud environments and remote-access enabled interfaces.
- Deploy a robust security framework around the migration and implementation of new cloud workloads.
- Stress test configurations and enhance the protection of the traditional perimeter (e.g., VPN, terminal emulation, VDI) and the "new" network perimeter (BYOD and "out of band" networks).
- Optimize security around messaging and communication applications (VC, email, instant messaging, etc.).

LAYERED SECURITY - DiD

- There is a need to protect the organization from advanced attacks using Multi Layered Security Approach – aka: **Defense in Depth**



CYBERTEAM 360
protecting what matters

WHAT IS YOUR CURRENT SECURITY STATUS?

For example: CyberTeam360 has created a simple but effective tool to provide a quantitative estimate of your current security status (including RA) and the development of a totally customized treatment plan. Tailoring your organization its own security-suit.

- The following threats are reviewed:

Attacks through vulnerable remote access

Attackers using stolen credentials

Unauthorized cloud access

Lost or stolen devices

Attacks through vulnerability in remote host

Man-in-the middle attacks

Data exfiltration & leakage

Capacity Issues

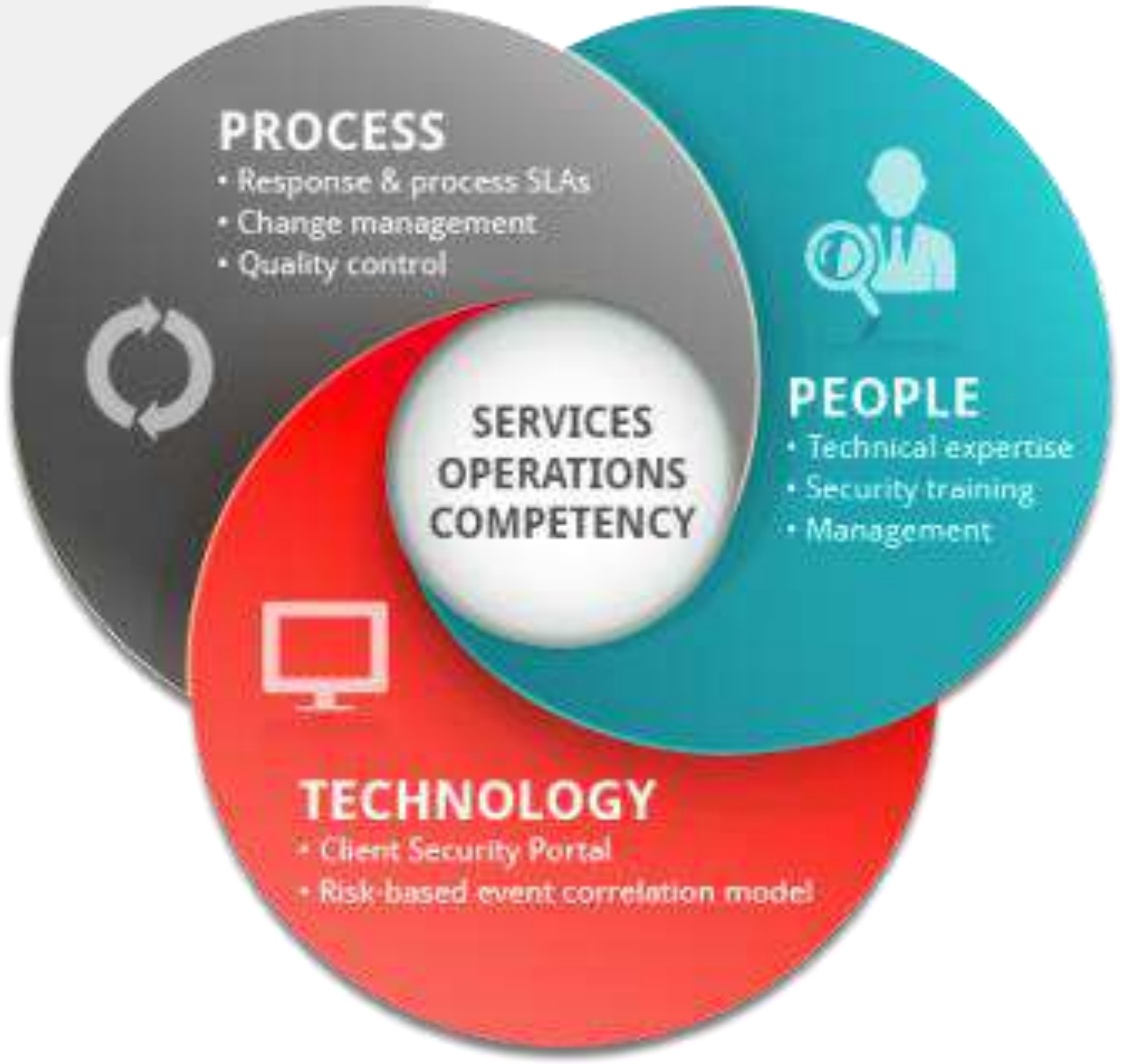
Data disclosure

CYBERTEAM 360
protecting what matters

CYBERSECURITY HEALTH STATUS

- The developed **“Quick Cyber Security Assessment”** tool , that once completed, will provide you with an assessment regarding your Information Security Program current status:

- Awareness of the cyber security
- Business continuity
- Governance
- Incident response
- Monitoring



PROCESS
- Response & process SLAs
- Change management
- Quality control

PEOPLE
- Technical expertise
- Security training
- Management

TECHNOLOGY
- Client Security Portal
- Risk-based event correlation model

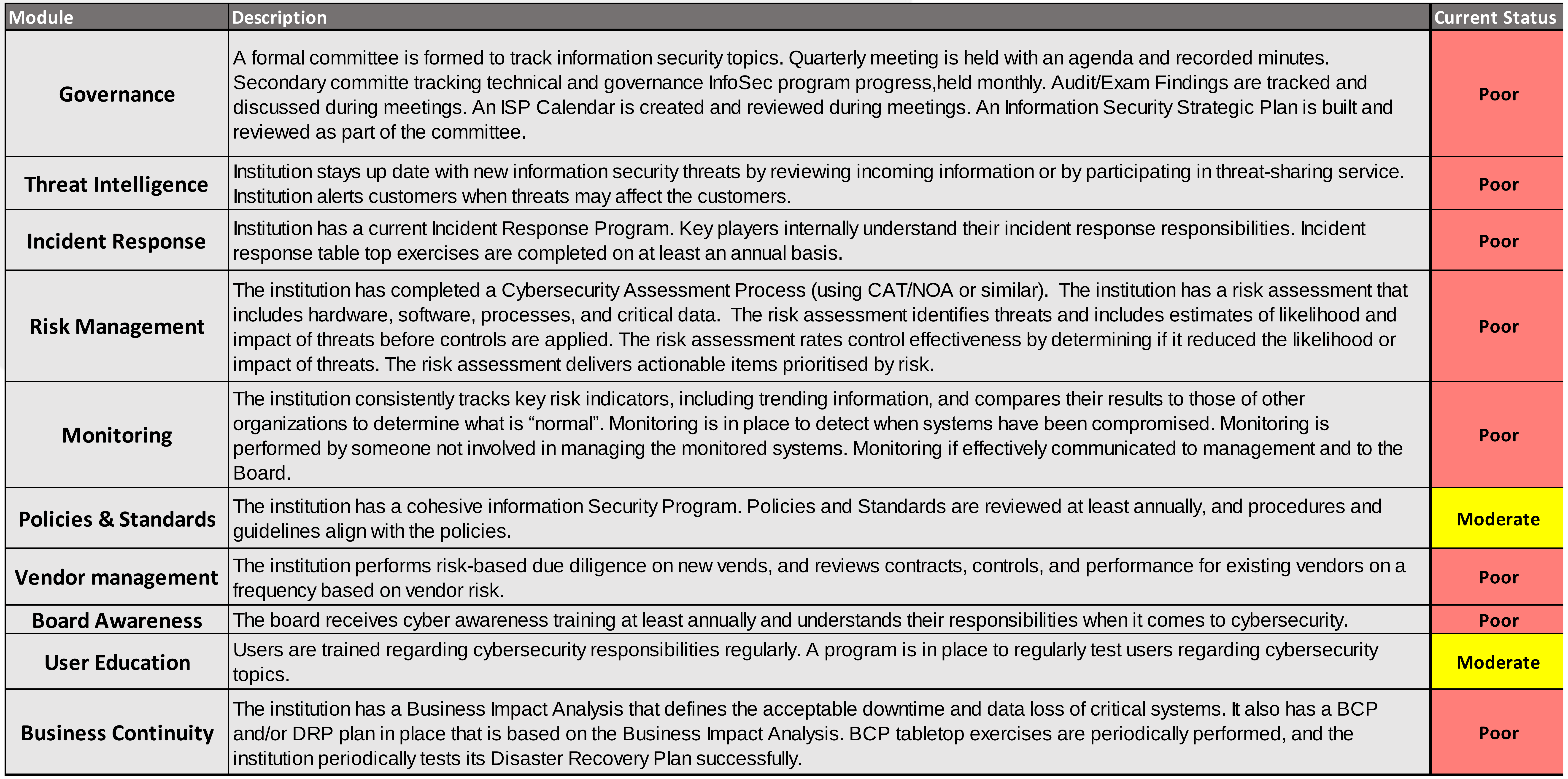
SERVICES OPERATIONS COMPETENCY

- Policies and Standards
- Risk Management
- Threat intelligence
- User education
- Vendor management

CYBERTEAM 360
protecting what matters

EXAMPLE OUTPUT

- Cyber Security Health Status – presenting your current security level and roadmap

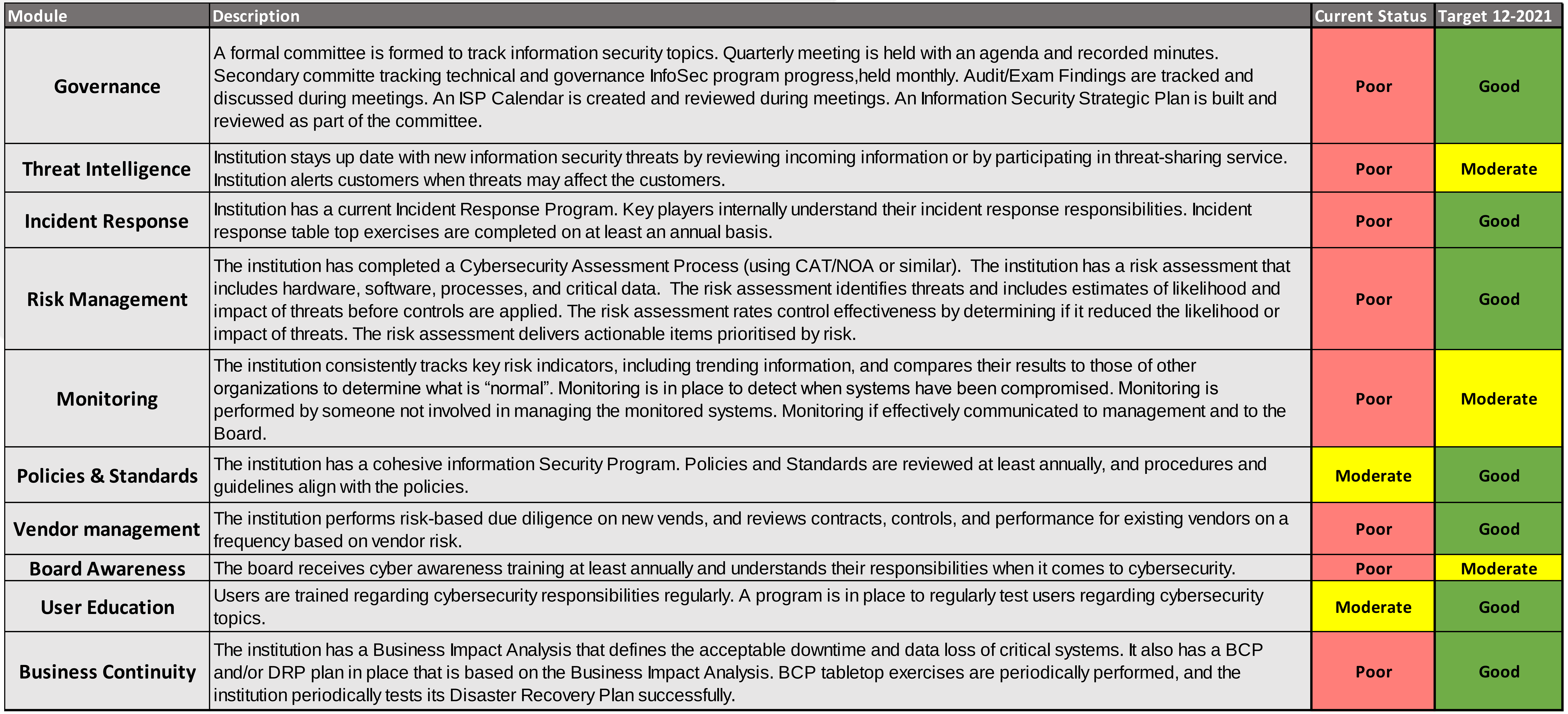


Module	Description	Current Status
Governance	A formal committee is formed to track information security topics. Quarterly meeting is held with an agenda and recorded minutes. Secondary committe tracking technical and governance InfoSec program progress,held monthly. Audit/Exam Findings are tracked and discussed during meetings. An ISP Calendar is created and reviewed during meetings. An Information Security Strategic Plan is built and reviewed as part of the committee.	Poor
Threat Intelligence	Institution stays up date with new information security threats by reviewing incoming information or by participating in threat-sharing service. Institution alerts customers when threats may affect the customers.	Poor
Incident Response	Institution has a current Incident Response Program. Key players internally understand their incident response responsibilities. Incident response table top exercises are completed on at least an annual basis.	Poor
Risk Management	The institution has completed a Cybersecurity Assessment Process (using CAT/NOA or similar). The institution has a risk assessment that includes hardware, software, processes, and critical data. The risk assessment identifies threats and includes estimates of likelihood and impact of threats before controls are applied. The risk assessment rates control effectiveness by determining if it reduced the likelihood or impact of threats. The risk assessment delivers actionable items prioritised by risk.	Poor
Monitoring	The institution consistently tracks key risk indicators, including trending information, and compares their results to those of other organizations to determine what is "normal". Monitoring is in place to detect when systems have been compromised. Monitoring is performed by someone not involved in managing the monitored systems. Monitoring if effectively communicated to management and to the Board.	Poor
Policies & Standards	The institution has a cohesive information Security Program. Policies and Standards are reviewed at least annually, and procedures and guidelines align with the policies.	Moderate
Vendor management	The institution performs risk-based due diligence on new vends, and reviews contracts, controls, and performance for existing vendors on a frequency based on vendor risk.	Poor
Board Awareness	The board receives cyber awareness training at least annually and understands their responsibilities when it comes to cybersecurity.	Poor
User Education	Users are trained regarding cybersecurity responsibilities regularly. A program is in place to regularly test users regarding cybersecurity topics.	Moderate
Business Continuity	The institution has a Business Impact Analysis that defines the acceptable downtime and data loss of critical systems. It also has a BCP and/or DRP plan in place that is based on the Business Impact Analysis. BCP tabletop exercises are periodically performed, and the institution periodically tests its Disaster Recovery Plan successfully.	Poor

CYBERTEAM 360
protecting what matters

EXAMPLE OUTPUT

- Cyber Security Health Status – presenting your current security level and roadmap



Module	Description	Current Status	Target 12-2021
Governance	A formal committee is formed to track information security topics. Quarterly meeting is held with an agenda and recorded minutes. Secondary committe tracking technical and governance InfoSec program progress,held monthly. Audit/Exam Findings are tracked and discussed during meetings. An ISP Calendar is created and reviewed during meetings. An Information Security Strategic Plan is built and reviewed as part of the committee.	Poor	Good
Threat Intelligence	Institution stays up date with new information security threats by reviewing incoming information or by participating in threat-sharing service. Institution alerts customers when threats may affect the customers.	Poor	Moderate
Incident Response	Institution has a current Incident Response Program. Key players internally understand their incident response responsibilities. Incident response table top exercises are completed on at least an annual basis.	Poor	Good
Risk Management	The institution has completed a Cybersecurity Assessment Process (using CAT/NOA or similar). The institution has a risk assessment that includes hardware, software, processes, and critical data. The risk assessment identifies threats and includes estimates of likelihood and impact of threats before controls are applied. The risk assessment rates control effectiveness by determining if it reduced the likelihood or impact of threats. The risk assessment delivers actionable items prioritised by risk.	Poor	Good
Monitoring	The institution consistently tracks key risk indicators, including trending information, and compares their results to those of other organizations to determine what is “normal”. Monitoring is in place to detect when systems have been compromised. Monitoring is performed by someone not involved in managing the monitored systems. Monitoring if effectively communicated to management and to the Board.	Poor	Moderate
Policies & Standards	The institution has a cohesive information Security Program. Policies and Standards are reviewed at least annually, and procedures and guidelines align with the policies.	Moderate	Good
Vendor management	The institution performs risk-based due diligence on new vends, and reviews contracts, controls, and performance for existing vendors on a frequency based on vendor risk.	Poor	Good
Board Awareness	The board receives cyber awareness training at least annually and understands their responsibilities when it comes to cybersecurity.	Poor	Moderate
User Education	Users are trained regarding cybersecurity responsibilities regularly. A program is in place to regularly test users regarding cybersecurity topics.	Moderate	Good
Business Continuity	The institution has a Business Impact Analysis that defines the acceptable downtime and data loss of critical systems. It also has a BCP and/or DRP plan in place that is based on the Business Impact Analysis. BCP tabletop exercises are periodically performed, and the institution periodically tests its Disaster Recovery Plan successfully.	Poor	Good

CYBERTEAM 360
protecting what matters

TIPS FOR EFFECTIVE AND SECURE REMOTE WORK DURING COVID-19 CRISIS

- Strengthen the access to your devices and users by using strong password authentication - ideally ***2FA apps / OTP sms*** (highly recommended).
- Define ***automatic locking*** after idle timeout. Select the shortest time possible as default threshold (for example 15 mins).
- Do not connect to a random Wi-Fi network that is not secured, prefer connection through VPN or cellular networks. If you can only connect from the home Wi-Fi network, make sure that the network is **private** and that a **complex password** is defined that is not the manufacturer's default.
- Usually the security level of the home router is weak and easy to breach. So it very important to take several simple steps to properly secure it (Updates, strong password and Secure Umbrella/OpenDNS config).

ADDITIONAL TIPS

- It is recommended to define automatic software updates in the operating system, and update the different software installed on the computers - this should be done routinely every 2 months (as a minimum).
- Make sure to have an up-to-date (and enabled…) ***antivirus*** **and** ***firewall*** software that are installed on the home computers.
- Instruct the employees to be alert for ***phishing attempts*** (all types of phishing) and to inform the authorized persons in the organization of any suspicion.
- It is obligatory to inform the authorized persons in the organization of any abnormal and suspicious event identified before and during connection to the organization.

MULTI-LAYERED SECURITY (DEFENSE-IN-DEPTH)

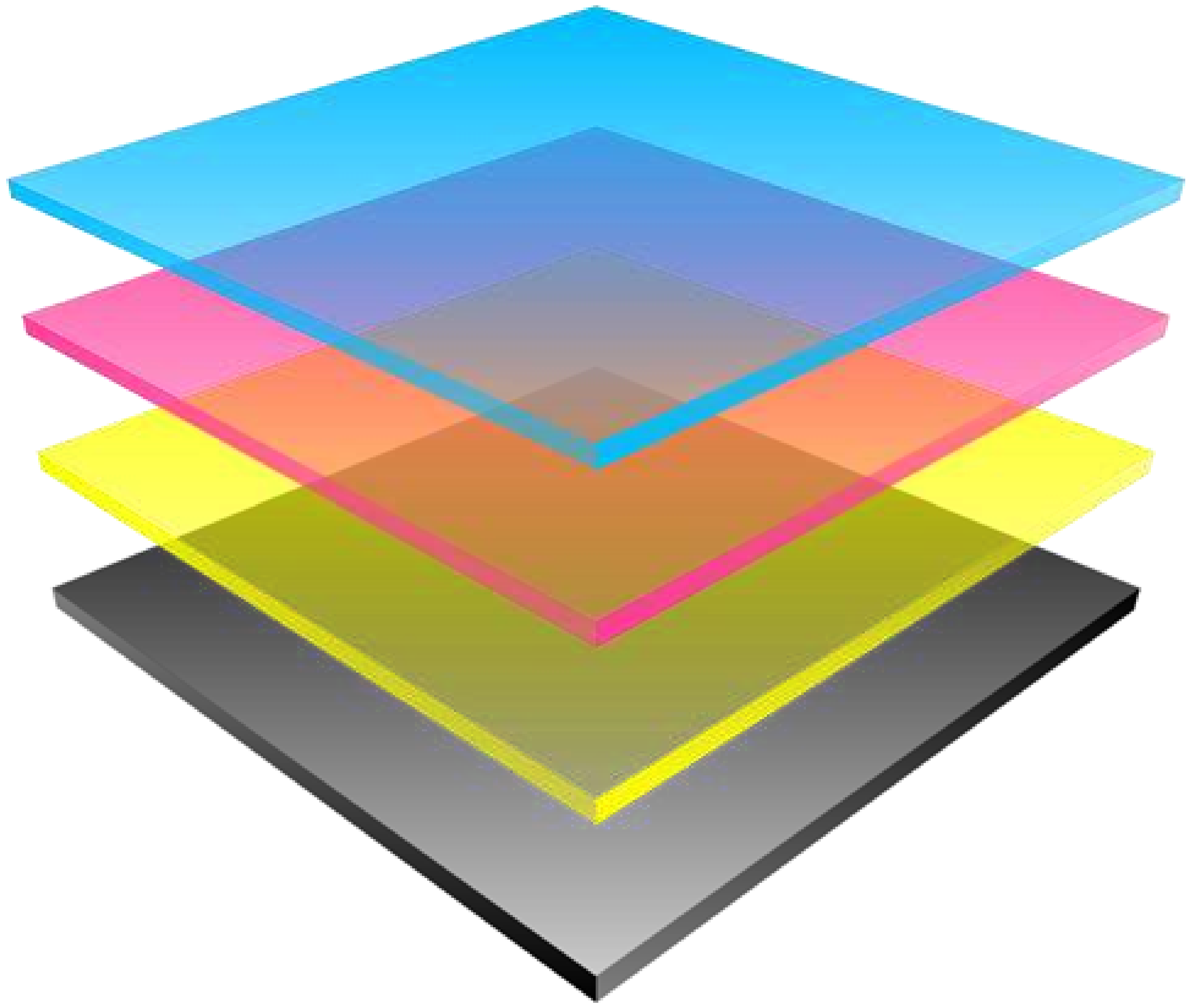
As a minimum you should:

TECHNOLOGY:

- Deploy antivirus protection or even better an EDR (Endpoint Detection & Response)
- Block and filter spam (Block risky file ext. (hta, js, vbs, chm etc…)
- Use a sandboxing solution
- Password protect backup & archive files
- Use URL filtering for Internet (block access to C&C servers)
- Use HTTPS filtering
- Use HIPS (host intrusion prevention) & other signature-less technologies
- Activate your client firewalls

PROCESS:

- Monitor for any unusual behavior
- Be vigilant and suspicious to every email
- Make sure to connect to your office remotely only from approve Internet/WiFi
- Use different passwords for your account and change frequently



REDUCE THE THREAT

Cyber Education

Backup & Encrypt Company Data

Use Advanced Security Tools

CYBERTEAM 360
protecting what matters

TIME FOR Q&A

I’ll be more than pleased to answer your questions!

Grazie mille

Thank you
for watching!

CYBERTEAM 360
protecting what matters