F&C CPAs

CYBERSECURITY & RISK

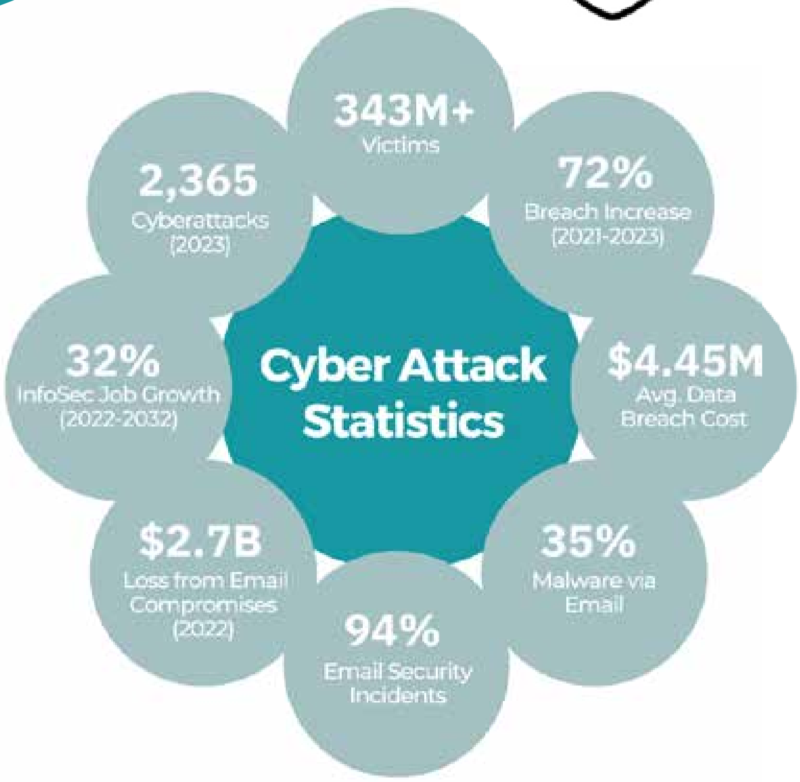
TRIBAL GAMING & ENTERPRISES
TRIBAL GOVERNMENTS & ENTTIES

Understanding the Crossroads

According to CISA, cybersecurity is the art of protecting networks, devices, and data from unauthorized access and ensuring confidentiality, integrity, and availability. Unlike science, cybersecurity constantly evolves, requiring creative solutions. Its dynamic nature demands tailored approaches to meet an organization's specific needs, as there is no single solution for all threats.

Risk involves exposure to potential danger, not the actual danger itself. It's the opportunity for something harmful to occur in your operations. The level of risk depends on the likelihood and impact of that danger. Every operation is unique, and each faces different risk factors based on its specific activities and environment, making risk management an essential, customized process.

For more information, visit Finley-Cook.com



Cyber Attack Statistics

343M+ Victims

72% Breach Increase (2021-2023)

$4.45M Avg. Data Breach Cost

35% Malware via Email

94% Email Security Incidents

$2.7B Loss from Email Compromises (2022)

32% InfoSec Job Growth (2022-2032)

2,365 Cyberattacks (2023)

Source:
St. John, Mariah. Feb 28, 2024. Cybersecurity Stats: Facts And Figures You Should Know.
Forbes Advisor. https://www.forbes.com advisor/education/it-and-tech/cybersecurity-statistics/

See page 2 for more info and contact details ℹ

TRIBAL GAMING,
GOVERNMENT, ENTITIES &
ENTERPRISE CAPABILITIES

RESPONSE TO RISK

As we understand and identify cyber-security risks, working through the response to those risks identified is equally important. There are four primary responses to identified risks:

1 Avoid

Avoiding risk may seem like the easiest solution, but in cybersecurity, it would mean not connecting to the internet at all—an unrealistic option. However, some specific activities can be avoided to reduce certain risks. When avoiding risk, it's important to weigh what is being sacrificed in the process.

2 Mitigate

Internal controls are designed to address identified risks. While they don't eliminate the risk, they help reduce its impact. In cybersecurity, most risks are mitigated through actions like strong passwords or extensive training, acknowledging that cyber-attacks are a constant threat that must be managed.

3 Share

Risk sharing, or transferring risk, happens when mitigation alone isn't enough. Cyber-attack insurance is a prime example, allowing organizations to share the financial burden of an attack despite having safeguards in place.

4 Accept

Sometimes, the best course of action is to accept certain risks, especially if mitigation isn't resource-efficient or sharing isn't possible. If the potential harm is minimal, accepting the risk can be the most practical approach.

Cybersecurity involves creatively protecting networks, devices, and data from unauthorized access and ensuring information confidentiality, integrity, and availability.

Understanding risk is crucial, as it represents exposure to potential danger rather than the danger itself, and it varies for each operation. By identifying and managing these risks, organizations can better protect themselves from cyber threats.

Let F&C help you navigate and respond to your unique cybersecurity risks effectively!

Tax Solutions

Compliance

Business Services

Advisory & Strategy

Training

Enterprise Technology

Scan to add
Doug to
your contacts

Doug Parker
TRIBAL SUPERVISOR

405-395-5106

405-401-9010

dparker@finley-cook.com

601 N. Broadway Avenue
Shawnee, OK 74801

F&C CPAs

FINLEY-COOK.COM

EXPLORE & SHARE

Scan to share to your
inbox or with a
colleague.