KROLL

When it comes to Cyber Security, Over Confidence is Costly

KROLL Cyber Risk – Elite Security Leaders Deliver End-to-End Solutions Worldwide

3,200+
ENGAGEMENTS IN 2021

650+ PRACTITIONERS ACROSS 18 COUNTRIES

100+
INDUSTRY CERTIFICATIONS (CISA, CRISC, CISSP, PFI, QSA, GPEN, CREST, OSCP, OSCE, ETC.)

FORTUNE 100 TO MEDIUM-SIZED BUSINESSES

PREFERRED / APPROVED VENDOR FOR **60+** CYBER INSURANCE CARRIERS

END-TO-END CAPABILITIES

GOVERNANCE
RESPONSE
ASSESSMENT
NOTIFICATION
MANAGED SECURITY

UNIQUE EXPERIENCE

GCHQ

INTERPOL

Recent Recognitions

SEP

Gartner

Recognized in Digital Forensics and Incident Response **(3rd Year)**

OCT

Gartner

Recognized in Managed Detection and Response (Kroll Responder)

Jason Smolanoff #5 in Top 50 Cyber Leaders of 2021 by **Consulting Report**

NOV

IDC

Named a leader in Incident Readiness

DEC

2021 Computing Security Awards WINNER

Winner:

Incident Response and Investigation Security Service

New Cloud Delivered Security Solution

Runner-Up:
Remote Monitoring Security Solution

FEB

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

7 Cyber Security Excellence Awards

- Managed Detection and Response
- Incident Response
- Breach Notification
- Breach and Attack Simulation
- Penetration Testing
- Red Teaming
- Virtual CISO

FORRESTER®

Named Strong Performer in Incident Response

APR

3 Cyber experts nominated for **Relativity Innovation Awards**

RELATIVITY INNOVATION AWARDS CUSTOMER EXPERIENCE 2022 AT RELATIVITY FEST

JUN

Advisen A ZYWAVE COMPANY

Won **Cyber Event Response Team of the Year**

Kroll Responder Won **Best Managed Security Service**

SC 2022 awards EUROPE

KROLL

Cyber Risk and CFOs: Over-Confidence is Costly

Introduction

Our research has shown that CFOs are highly confident in their companies' abilities to ward off cyber security incidents, despite being somewhat unaware of the cyber vulnerabilities their business faces. Almost 87% of the surveyed executives expressed this confidence, yet 61% of them had suffered at least three significant cyber incidents in the previous 18 months. Moreover, they admitted to being out of the loop: 6 out of 10 were not regularly briefed by the cyber team, and nearly 4 out of 10 had never received such an update, according to the survey conducted by Kroll and studioID of Industry Dive.

The CFOs also put a price tag on the cyberattacks they had suffered in the previous 18 months: between $10 million and $25 million for about one-third of companies who suffered a significant security incident, and more than $25 million for almost 16% of the companies. It is imperative that CFOs and their finance teams up their involvement in cyber investment, from planning to prevention and response strategies. Failing to do this leaves CFOs out of the loop on cyber issues and threatens the business with significant—and, critically, unexpected—financial consequences.

Key Points

- A total of 87% of CFOs are confident in their companies' cyber security capabilities but 4 out of 10 had never had a briefing from information security leadership
- Comparatively, 66% of Chief Information Security Officers (CISOs) in the State of Incident Response 2021 report thought that their organization was vulnerable, and 82% said that the average organization in their industry was vulnerable to cyberattack
- 71% have suffered more than $5 million in financial losses stemming from cyber incidents in the last 18 months
- 82% of the executives in the survey said their companies suffered a loss of valuation of 5% or more following their largest cyber security incident in the last 18 months
- Cyber security spending is increasing; 45% of respondents plan to increase the percentage of their overall IT budget dedicated to information security by at least 10%
- CFOs need to understand cyber security strategies and the resulting investments required, as well as potential financial risks from cyber incidents

KROLL

Cyber Risk and CFOs:

Over-Confidence is Costly

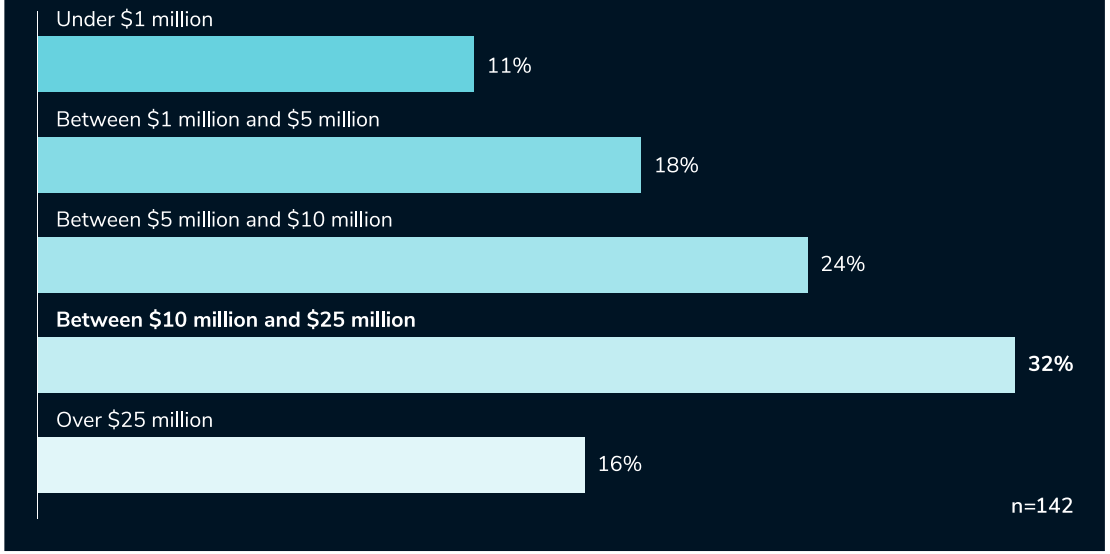
2022 Edition

Cyber Risk:

The financial impact of cybersecurity

A recent Kroll survey shows 87% of CFOs are highly confident in their companies' cyber defenses, **but** 61% suffered at least three incidents in the last 18 months.

Most (56%) reported between $5 and $25M as the total financial impact of cyber incidents in the last 18 months



Organizations suffered damage across a wide spectrum of impact areas, including:

- Cyber and privacy counsel costs
- Crisis communications, customer notification
- Insurance premium increase
- Impairment of brand, IP or goodwill
- Regulatory penalties
- Damage to reputation

Download the full report:
Cyber Risk and CFOs: Over-Confidence is Costly

https://www.kroll.com/-/media/kroll-images/pdfs/cyber-risk-cfos.pdf

KROLL

Cyber Risk:

The financial impact of cybersecurity - EMEA

- It seems that CFOs in EMEA are much more involved with the cyber security team

- 40% of CFOs briefed monthly by their information security teams, compared to 24% globally.

- Despite suffering less incidents in the last 18 months - 43% of respondents in EMEA, compared to 61% globally – they were less confident (28% compared to 53%) in their company's ability to respond to a cyberattack.

Download the full report:
Cyber Risk and CFOs: Over-Confidence is Costly

https://www.kroll.com/-/media/kroll-images/pdfs/cyber-risk-cfos.pdf

KROLL


Q2 2022 Threat Landscape: Ransomware Returns, Hea
Q2 2022 Threat Landscape:
Ransomware Returns, Healthcare Hi
Authors
Laurie Iacono
Keith Wojcieszek
George Glass
In Q2 2022, Kroll observed a 90% increase in the number of healthcare organizations targeted in comparison with Q1 2022, dropping the final nail in the coffin for the "truce" some criminal groups instituted earlier in the COVID pandemic. Ransomware helped to fuel this uptick against healthcare as attacks increased this quarter to once again become the top threat, followed closely by email compromise.
While Kroll continued to see actors exploiting vulnerabilities and phishing schemes to launch ransomware, in Q2 a ransomware incident was most likely to begin via external remote services. Kroll observed a 700% increase in external remote services such as remote desktop protocol (RDP) and virtual private networks (VPN) being used for initial access in the quarter. Of ransomware incidents beginning with phishing, Kroll observed an uptick in the use of Qakbot malware as a delivery mechanism, particularly for new ransomware groups like Black Basta.
The recent shift to targeting the healthcare industry comes alongside the persistence of ransomware as an incident type and the rise in external remote services being used as an initial access method, giving us an indication of where attackers may focus in coming months. All organizations—especially those in healthcare— would do well to test the resilience of their external remote services and preparedness for ransomware.
Most Popular Threat Incident Types - Past Three Quarters
40%
32%
33%
27%
32%
30%
22%
17%
26%
6%
9%
Ransomware
Email Compromise
Unauthorized Access
Web Compromise
Q4 2021
Q1 2022
Q2 2022
KROLL
Q2 2022
Threat Landscape:
Ransomware Returns,
Healthcare Hit

Cyber Risk:

Reasons for investing in cybersecurity

Q2 2022:

Ransomware and Email Compromise were the top threat incident types in Q2, with Ransomware incidents increasing from the first quarter.

700% increase in external remote services such as remote desktop protocol (RDP) and virtual private networks (VPN) being reported for initial access.

Uptick in the use of Qakbot malware as a delivery mechanism, particularly for new ransomware groups like Black Basta.

90% increase in attacks against the health care sector due to an increase in ransomware and unauthorized access.

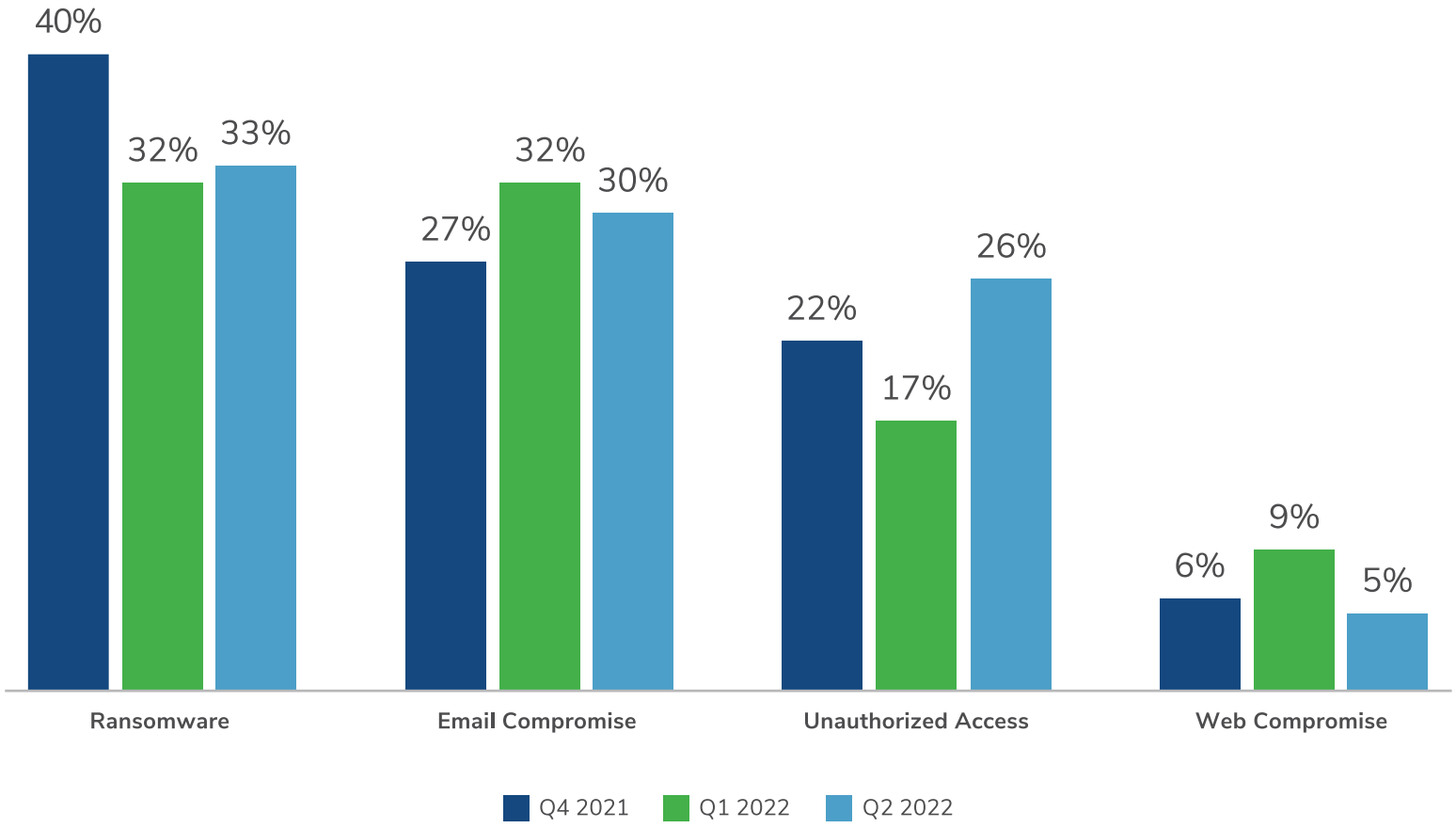
Download the full report:
Q2 2022 Threat Landscape: Ransomware Returns, Healthcare Hit

KROLL

Cyber Risk:

Most Common Threats

Ransomware and email compromise remain most common causes of cyber incidents, often leading to extensive data theft and privacy / regulatory concerns

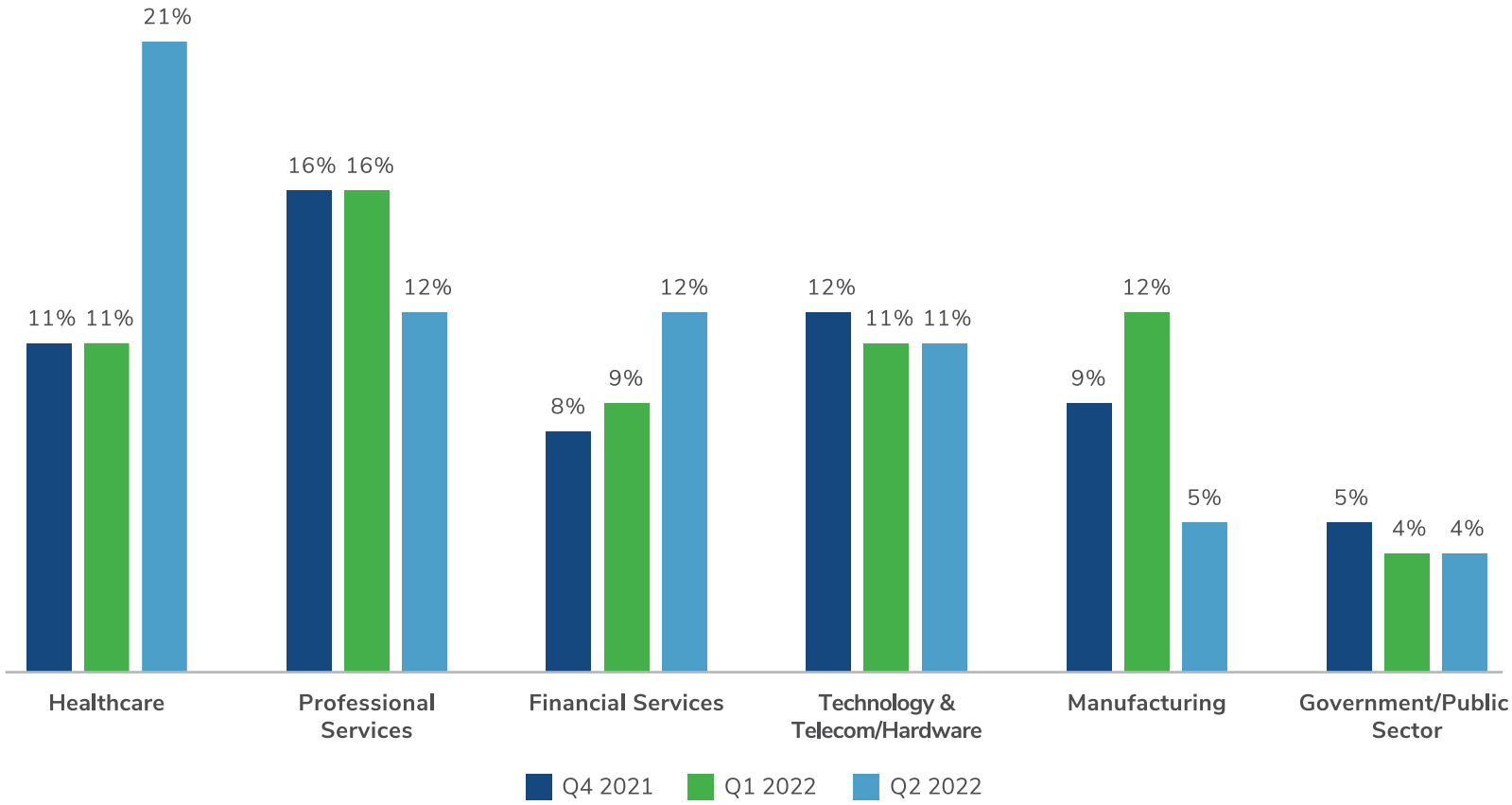


KROLL

Cyber Risk:

Most Targeted Industry Sectors

Professional, financial services and technology sectors consistently targeted



KROLL


KROLL
Q3 2002
Threat Landscape:
Insider Threat,
The Trojan Horse
of 2022

Breaking Research

The rise of Insider Threat

THIS QUARTER:

We saw insider threat peak to its highest level yet, with it almost doubling in volume compared to the second quarter of the year. Insider threat makes up part of the unauthorized access category, which underwent an increase in popularity as a threat incident type from 15% in Q2 to 22% in Q3.

Kroll also observed a number of malware infections via USBs in Q3, suggesting that wider external factors such as an increasingly fluid labor market and widespread economic turbulence may encourage insider threat.

Join the webinar in EMEA on **November 8, 2022**
Register Now

KROLL

KROLL

Thank You

KROLL

For more information, please contact:

Carlos García

Senior Vice President

+34 655 595 144

carlos.garcia@kroll.com

For immediate 24x7 support from Kroll's global team of Cyber Risk experts, visit our website or call the hotlines listed below.

EMEA

+44 (0) 808 101 2168 (toll free)

www.kroll.com/es-es

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.