New York Bankers Association

Financial Services Forum

Naples, FL
November 1, 2022

75-min presentation by

ARCTIC WOLF

Today’s theme:

What’s going on in the Cyber World that the C-suite needs to know about

Focus areas:

- Cyber Incident Trends
- Focus on MFA
- Political and Regulatory Pressures
- Cyber Culture within your Bank

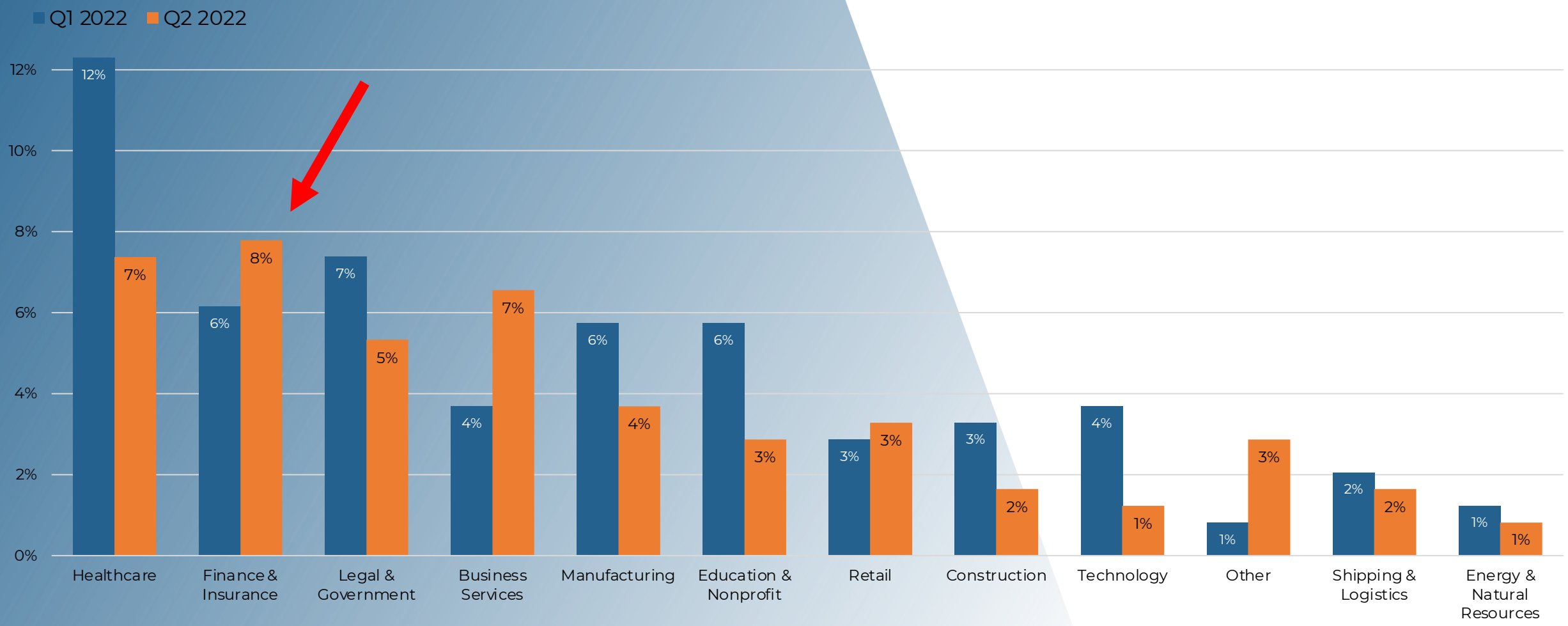
Topic 1

Cyber Incident Trends

This data summarizes aggregated and anonymized information related to **Incident Response (IR) cyber insurance claims** that Arctic Wolf investigated from January – June 2022

INCIDENTS BY INDUSTRY

Investigations during January – July 2022



RANSOMWARE ROOT POINT OF COMPRIMISE (RPOC) BY INDUSTRY

Q1 & Q2 2022

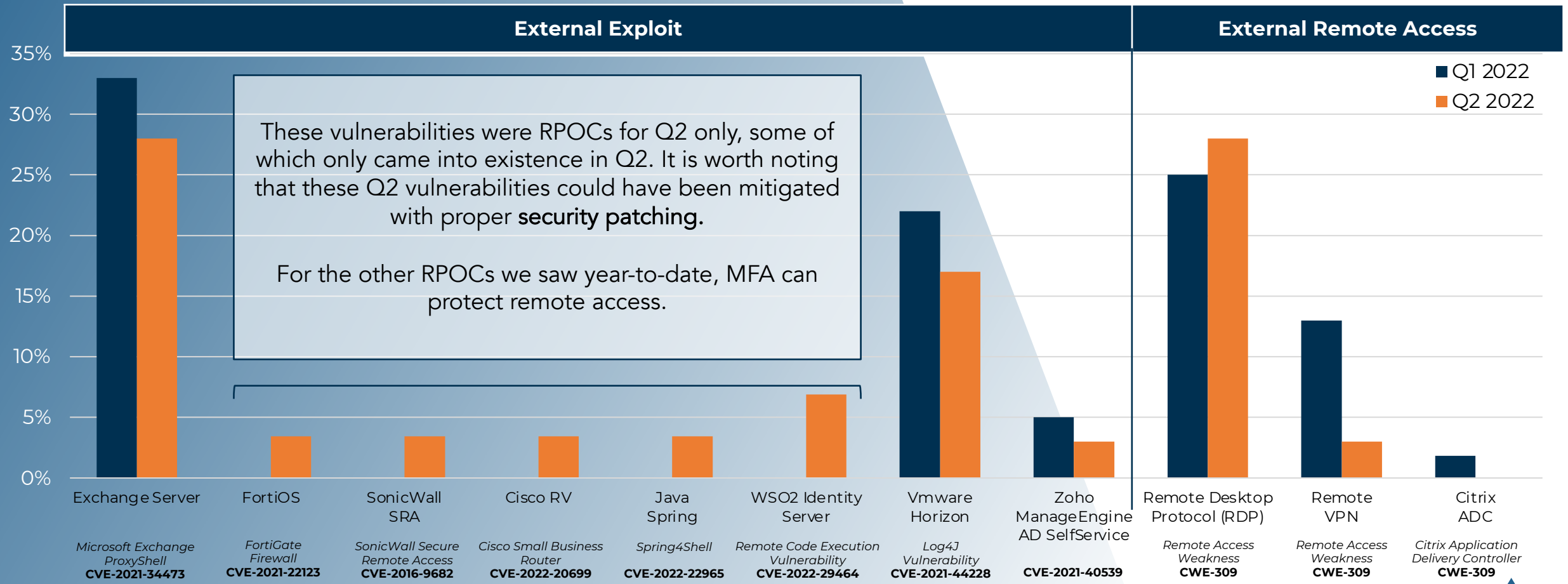
Sorted by Case Volume by Industry

Industry	External Exposure		User Action		
	External Exploit	External Remote Access	Phishing Email	Social Engineering	Drive by Attack
Healthcare	61%	35%			4%
Finance & Insurance	33%	25%	17%	8%	17%
Legal & Government	60%	10%	30%		
Business Services	14%	43%	29%	14%	
Manufacturing	70%	10%	10%		10%
Education & Nonprofit	69%	23%		8%	
Retail	60%	40%			
Construction	50%	25%	25%		
Technology	67%	33%			
Other	100%				
Shipping & Logistics	80%			20%	
Energy & Natural Resources			100%		

RANSOMWARE RPOC BY PRODUCT

Q1 & Q2 2022

Threat actors carried out the majority of attacks via **vulnerabilities** and weaknesses they know how to exploit. The following are products / vendors leveraged in Arctic Wolf cyber insurance incident response work so far this year.



Topic 2

Focus on MFA

§ 500.12(b)

According to the DFS, MFA weaknesses are the most common cybersecurity gap exploited at financial services companies.

From January 2020 to July 2021, **64% of entities regulated by DFS that reported a cybersecurity incident had some sort of gap in MFA.**

Over 18.3 million consumers were impacted by cybersecurity incidents reported to the DFS **by** companies with **MFA failures.**

Source: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance

Most common MFA issues seen by NYS DFS*

- Legacy systems that don’t support MFA
- Gaps in coverage for remotely-accessible apps
- Third-party access
- Incomplete MFA rollouts
- Unjustified MFA exceptions

* Arctic Wolf is also seeing an increase in MFA fatigue attacks (Uber for example)

Sources: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance & https://arcticwolf.com/resources/blog/growing-risk-of-mfa-fatigue-attacks/

Topic 3

Political and Regulatory Pressures

Ukraine/Russia Conflict & multi-million-dollar DFS fines

“The Russian invasion of Ukraine significantly elevates the cyber risk for the U.S. financial sector. ” – NYS DFS

Political Pressures

> “Escalating tension between the U.S. and Russia also increases the risk that Russian threat actors will directly attack U.S. critical infrastructure in retaliation for sanctions or other steps taken by the U.S. government.” – NYS DFS

- Review MFA hygiene
- Test Incident Response Plans – what’s your plan for ransomware negotiation, digital forensics, and recovery?
- Review backups – can they withstand ransomware?
- Additional cyber awareness training
- Monitor/inspect/isolate traffic from Russia / Ukraine
- Report incidents within 72 hours per 23 NYCRR §500.17(a)

Source: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220225_ukraine_escalation_impact_financial

Regulatory Pressures

- DFS Fines:
  - March 2021 - $1.5m – Residential Mortgage Services – hiding a cyber breach and failing to report it
  - July 2022 - $5m – Carnival – cyber breach with improper attestation of compliance
  - August 2022 –$30m – Robinhood – bank secrecy and cybersecurity violations

Source: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220225_ukraine_escalation_impact_financial

Regulatory Pressures - July 29 ‘22 Proposed Amendments

- For Larger Banks (“Class A”)
  - Applies to banks with 2,000+ employees, or
  - $1bn in average revenue over last 3 years

- Conduct systematic scans or reviews at least weekly (vs. bi-annually)
- Increased CISO responsibilities – Authority to make binding decisions about cybersecurity program
- Independent cybersecurity audits (not an audit by the person doing the work)
- MFA for all privileged accounts

Source: Search for “pre_proposed_draft_23nycrr500_amd2.pdf”

Topic 4

Cyber Culture within your Bank

88% of boards regard cybersecurity as a business risk rather than solely a technical IT problem. – Gartner

Source: https://www.gartner.com/doc/reprints?id=1-29FBE5ZT&ct=220317&st=sb

Cyber Culture within your Bank

Gartner's Key Findings:

- Finding: Executive performance evaluations are increasingly linked to an ability to appropriately manage cyber risk within their parts of the business.

- Finding: Expectations that organizations should be more transparent about their security risks have increased.

Source: https://www.gartner.com/doc/reprints?id=1-29FBE5ZT&ct=220317&st=sb

Cyber Culture within your Bank

Gartner's Key Predictions:

- Prediction: By 2026, at least 50% of C-Level executives will have performance requirements related to cybersecurity risk built into their employment contracts.

- Prediction: By 2025, 40% of programs will deploy socio-behavioral principles (such as nudge techniques) to influence security culture across the organization, up from less than 5% in 2021.

Source: https://www.gartner.com/doc/reprints?id=1-29FBE5ZT&ct=220317&st=sb

THANK YOU

FOR FOLLOWUP, PLEASE CONTACT:

JEFF MILLER

518-390-2534 (CELL)

JEFF.MILLER@ARCTICWOLF.COM