Cyber Risk Management

johnson
kendall
johnson

JKJ

Insurance & Risk Management Brokerage

- Formed in 1959 - 60 years of Experience
- Founder of the 401k
- *Independently-Owned*
- Clients in multiple industries across 43 states & internationally

Commercial Insurance

Global Solutions

Employee Benefits

Personal Insurance

Financial Services

Retirement Services

CERTIFIED

EVERGREEN

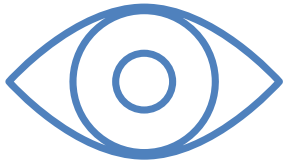
JKJ Experience in Non-Profit

- Proud to have one of the largest client portfolios in nonprofit human services & senior living organizations in the country including:

• Intellectual, Behavioral & Development Disability Services	• Children & Family Services	• Schools & Athletic Programs
• Drug & Alcohol Rehabilitation Facilities	• Mental Health Agencies	• Medical Clinics
• Long-term care facilities	• Nursing Homes	• Residential Care
• Vocational Services	• Continuing Care Retirement Communities	• And more…

- Insured the first CCRC in PA in 1968 – still a client to this day

JKJ Vision



- To create a service driven, risk management platform such that JKJ becomes an extension of our clients' Insurance and Risk Management Team.
- Our Focus
  - Risk Prevention (Loss Control)
  - Risk Transfer (Insurance and/or Contractual)
  - Risk Mitigation (Claims Management)
  - Continually develop risk management programs that will avail the tools to reduce losses

Speaker Information

Alexandra H. Bretschneider, CCIC
Cyber Practice Leader, Vice President

- St Joseph's University – MIS & Finance
- Big 4 IT Consulting & Telecom Consulting Background
- *Cyber COPE Insurance Certification* from Carnegie Mellon Heinz College of Information Systems & Public Policy
- Founded JKJ's Cyber Practice
  - Awarded Cyber Broker of the Year 2021 by Advisen
  - Recognized as Cyber Unsung Hero 2022 by Advisen
  - Continually speaking at industry leading events & associations

JKJ Cyber Practice

Three Pillars of Service:

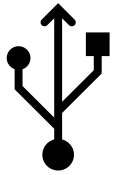
- **Preventative/Mitigation** – Cyber Security Controls Review, Network Scans, Social Engineering Theft Prevention, Education Resources, Incident Response Planning & Tabletop Exercises, IT Cybersecurity & Legal Partners
- **Risk Transfer/Insurance –** Contract Reviews, Coverage Analysis, Limit Assessments, Breach Calculators; Data Benchmarking
- **Incident Response –** expedited communication and action from Insurance carrier and critical resources from Legal and Forensics

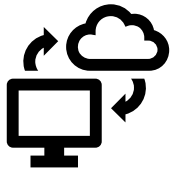
Agenda

- Trends
- Managing Cyber Risk
- Insurance Overview & Considerations
- Regulatory Changes
- Preparation

Cyber Incidents - Landscape

- Ransomware
- Theft of money
- Phishing Attack
- Data Breach
- Denial of Service Attack
- Lost or Stolen Device/Files
- Disclosure of Private Information
- Hacking
- Malware
- Vendor Error or Negligence
- Physical Security Breach
- The Unknown…





- It is estimated more than 50 billion devices and processes are connected to the internet
- Cybercrime cost $8.4 trillion in 2022.
- Impacts to businesses include compliance, operational, and financial.

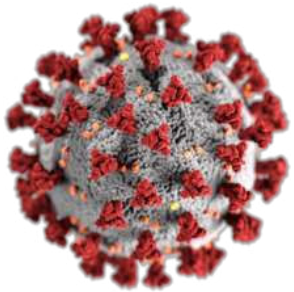
**Source: Statista Magazine*

CYBER CLAIM TRENDS

Data Breaches (Privacy)

Social Engineering ($)

Ransomware (Operations)



"Ransomware gangs don't care about your data, **you care about your data**, and that's why everyone is a target."

Scott Walsh, Senior Engineer, Coalition

By the numbers…

- **In 2020:**
  - Average extortion demand skyrockets to $100k+ and frequency of attacks increased exponentially
- **In 2021**
  - Average extortion demand continues to rise (by Q2 over $570k)
  - Businesses attacked by ransomware every 11 seconds.
  - Average downtime is between 19-23 days
  - The number of zero-day exploits doubled over 2020 – a key target for ransomware attacks, many of which impacted supply chains (IT and otherwise)
  - Multiple layers of extortion – network encryption, data release, harassment of clients & employees, printbombing
  - Federal/Regulatory Response – call for action nationally & internationally

Sources: https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/
Arete 2021 Crimeware Report

By the numbers…

- **2022:**
  - Phishing attacks increased by 48% in the first half of 2022
  - 40% of cyber threats are now occurring directly through the supply chain.
  - Internet of Things (IoT) continues to grow as a target for cybercriminals.
  - 98% of claims impact SMEs of less than $1B in revenue
  - Average downtime of a ransomware event – 24 Days
  - Ransomware – up or down in 2022? Depends who you ask and frequency vs. severity
  - Increased regulatory response

Sources: https://connect.comptia.org/blog/cyber-security-stats-facts#:~:text=Cybercrime%20Statistics%20by%20Attack%20Type&text=Phishing%20attacks%20increased%20by%2048,directly%20through%20the%20supply%20chain.; *NetDiligence 2021 Report*

2022 Cautiously Optimistic News

Cybercriminals Are More Likely Than Ever To Get Caught

Pricing pressures moderate as cyber insurance market begins to level out

A surge in new buyers has begun to offset years of rising claims and higher premiums, according to data from global insurance firm Marsh.

Published July 1, 2022

Ransomware activity falls 25% in Q1 2022

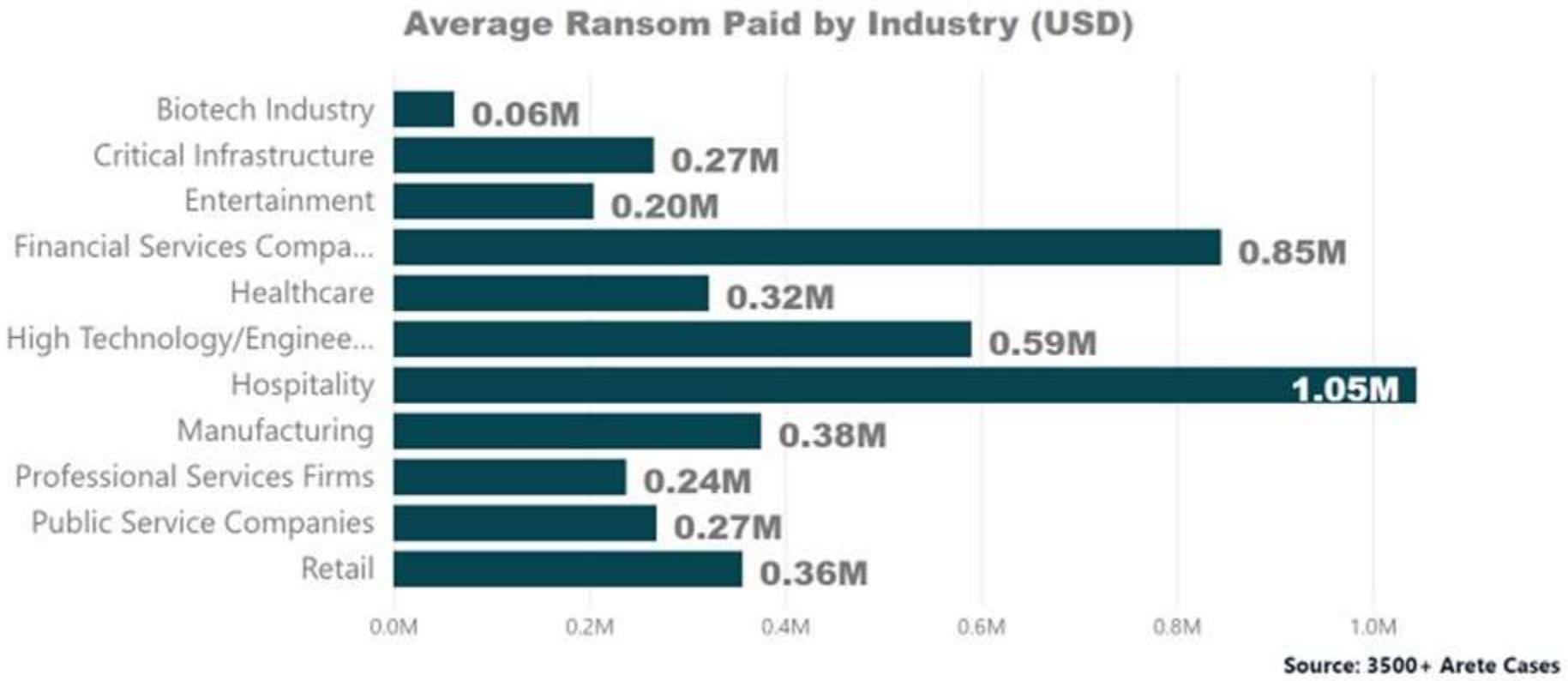
The drop in ransomware has been attributed to larger ransomware gangs being less active compared to the end of 2021

by: Connor Jones 14 Apr 2022

Ransomware Statistics

Source: Arete Crimeware Report

Ransomware Statistics

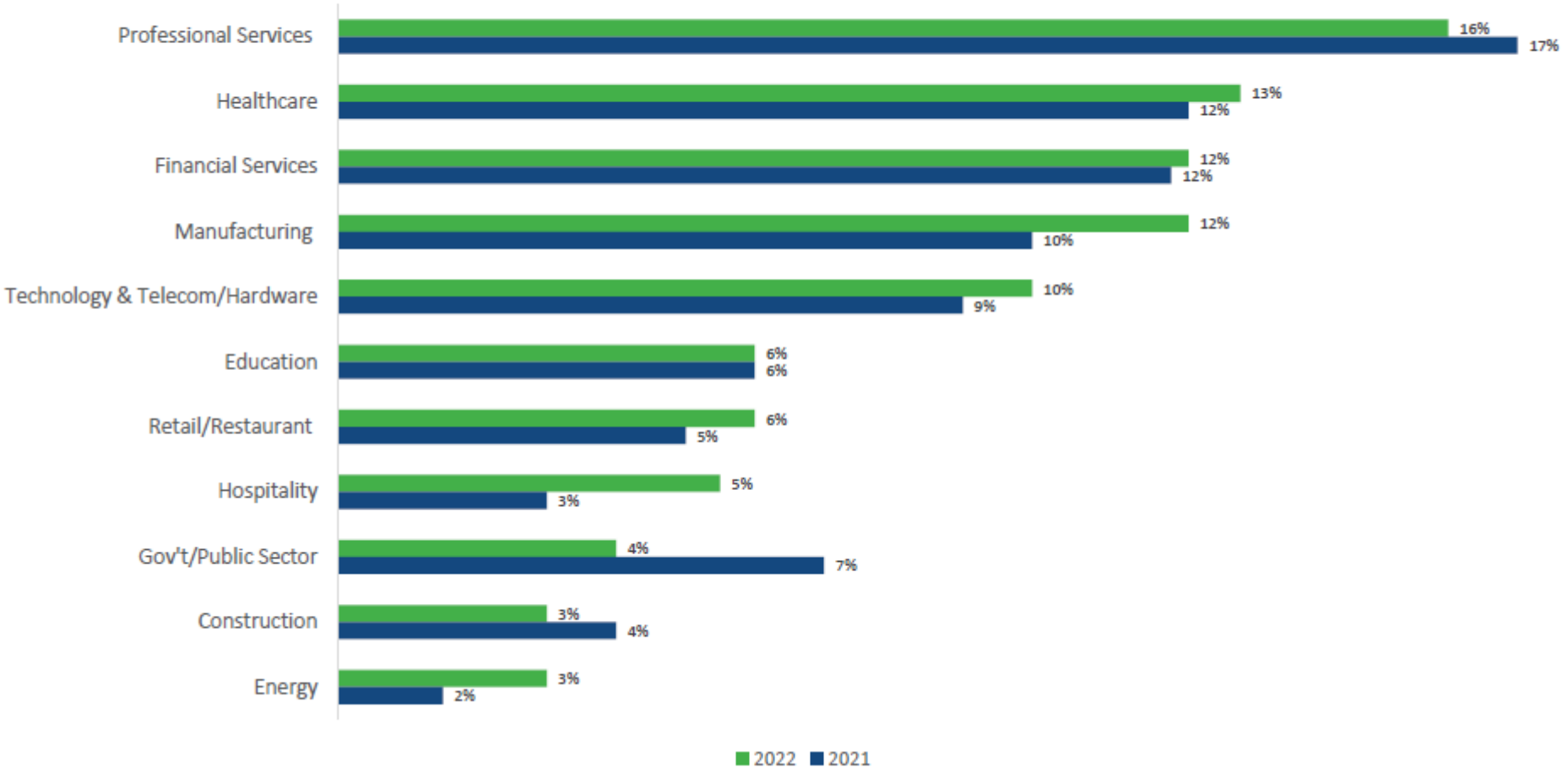


Source: Arete Crimeware Report

Who is being targeted?

Incidents by Sector

2021-2022 Comparison

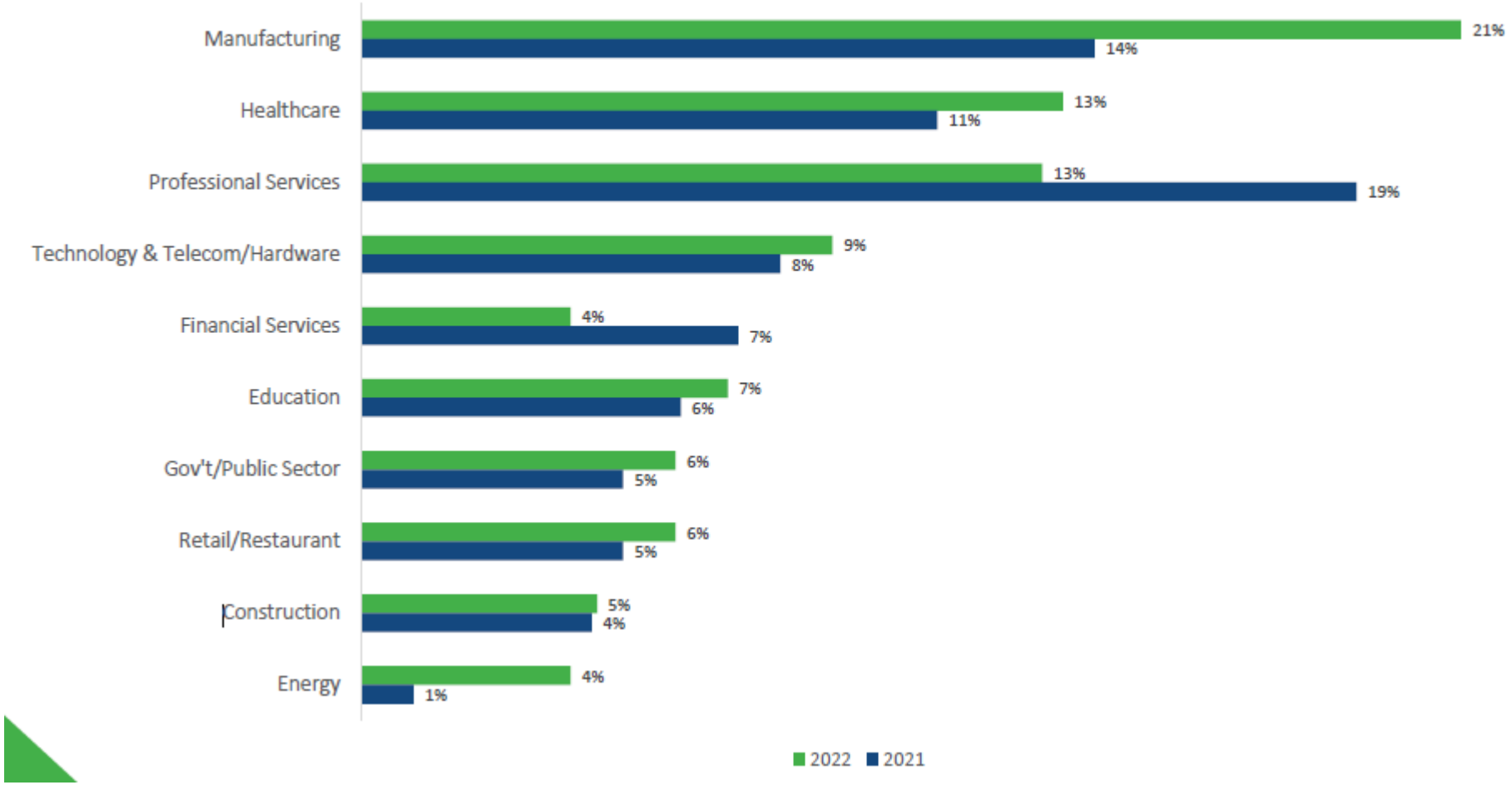


Source: Kroll 2022 Year-End Spotlight Report

Who is being targeted?

Ransomware – Top Impacted Sectors

2021-2022 Comparison

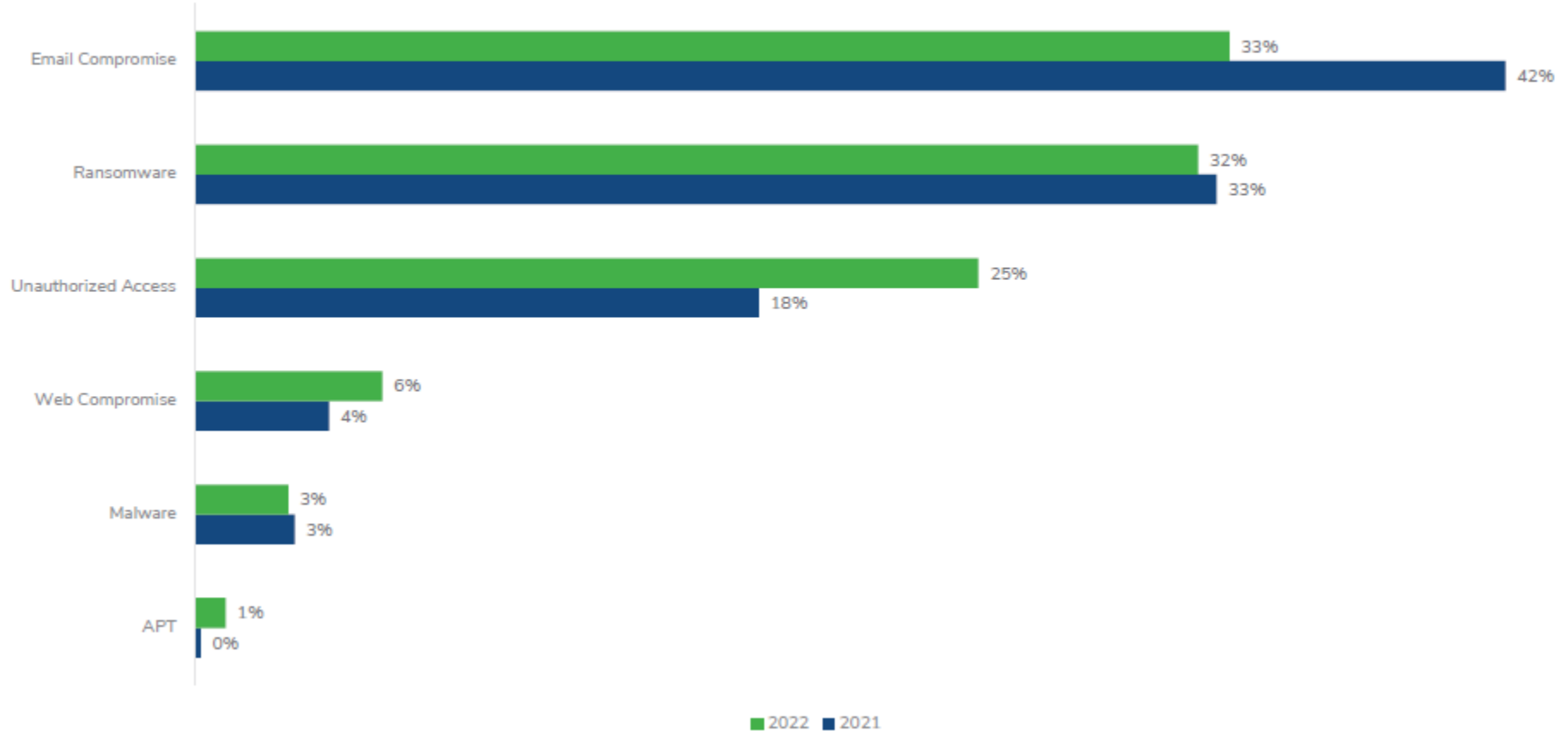


**Source: Kroll 2021 Year-End IR SpotlightTrends Report*

Threat Type

Incident by Threat Type

2021-2022 Comparison

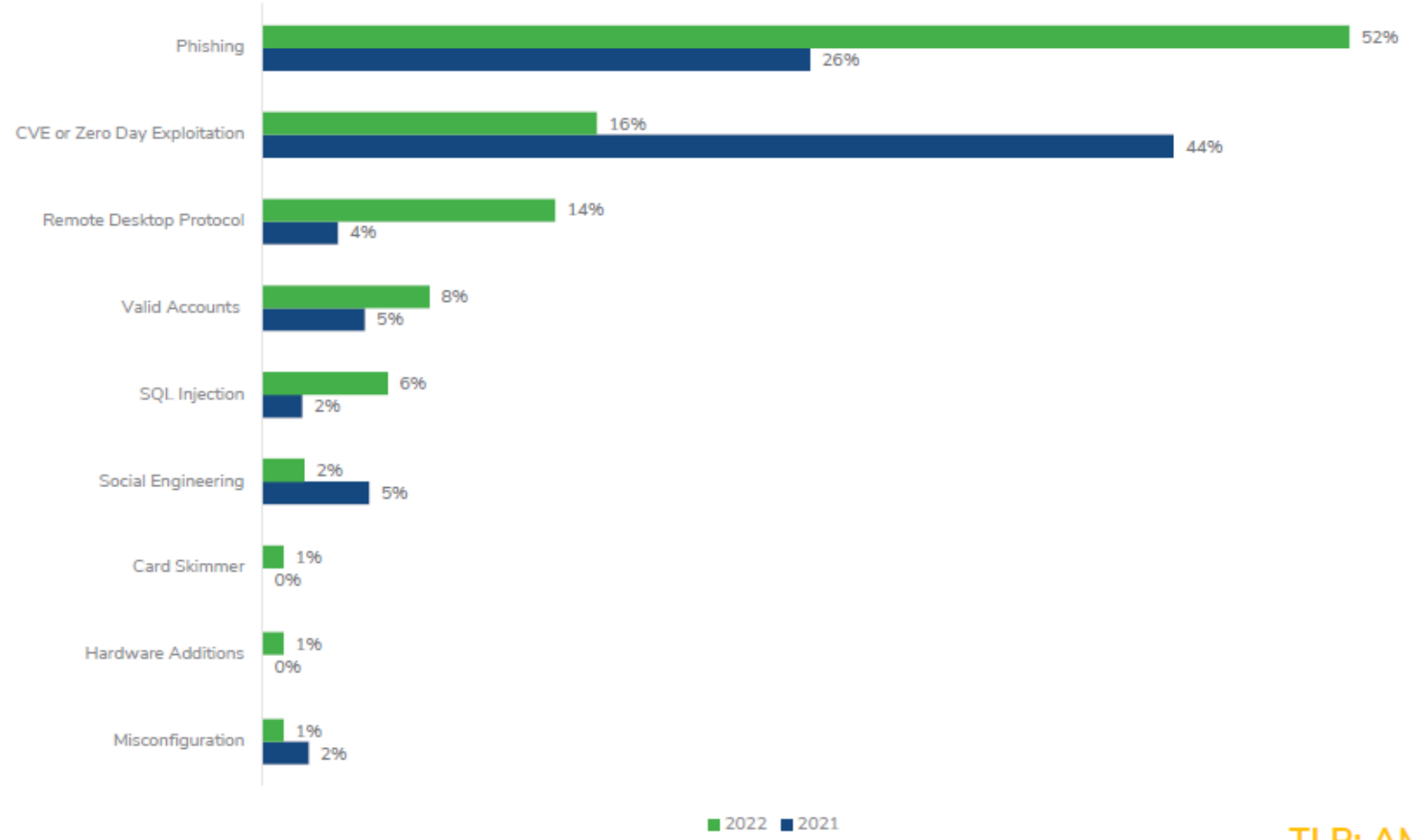


Source: Kroll 2021 Year-End IR SpotlightTrends Report

Who is being targeted?

Top Initial Access Methods

2021-2022 Comparison

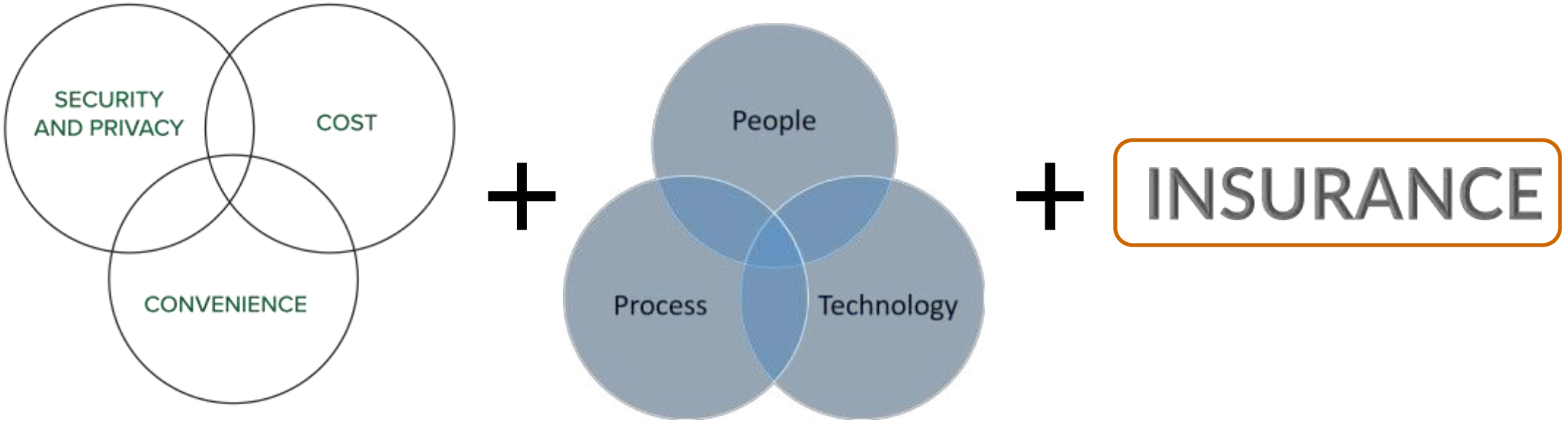


TLP: AMBER

*Source: Kroll 2021 Year-End IR SpotlightTrends Report

What can we do about it?

Cyber Risk Management



GOALS:

1. Reach a state of ***CYBER RESILIENCE*** in which you can properly identify, respond, and recover from a Cyber Incident.

2. Be cognizant of the ***REASONABLENESS STANDARD.***
    - What would I reasonably expect of a similar company?

Cyber – Supply Chain Risk Management

Key Considerations:
Vendor Management - IT and Non-IT vendors

- Inventory of Vendors
  - What do they have access to? (System and/or information)
  - How is access controlled?

- What do the contracts say?
  - Indemnification, Hold Harmless, Confidentiality, Responsibility
  - Insurance requirements

- Business Continuity/Disaster Recovery Planning

Role of Insurance in Incident Response

You	MSP/IT	Insurance	Legal	Forensics	FBI
• Decision making • Pay or not pay ransom? • Business continuity • Set priorities • Establish communication channels	• Triage • Support forensics data gathering • Restoration & Recovery of data and systems	• Bring in additional resources (legal, forensics) • Approve / manage costs • Prepare notification and credit monitoring resources • Determine coverage	• Breach Coach / Quarterback • Establish privilege • Represent legal and compliance obligations • Declare “breach”/”no breach” • Response leadership • Communication	• Determine the how and what (cause & scope) • Provide reporting and evidence to legal • Advise IT on securing the environment and restoration	• Assistance in conducting a criminal investigation • May involve collecting incident artifacts, to include system images and malware samples.
		Broker	**May engage Public Relations**		**May not participate**

Insurance (the fun stuff)

What is Cyber Insurance

A KEY PART OF YOUR CYBER RISK MANAGEMENT STRATEGY

Cyber Insurance is designed to cover the costs of a cyber incident.

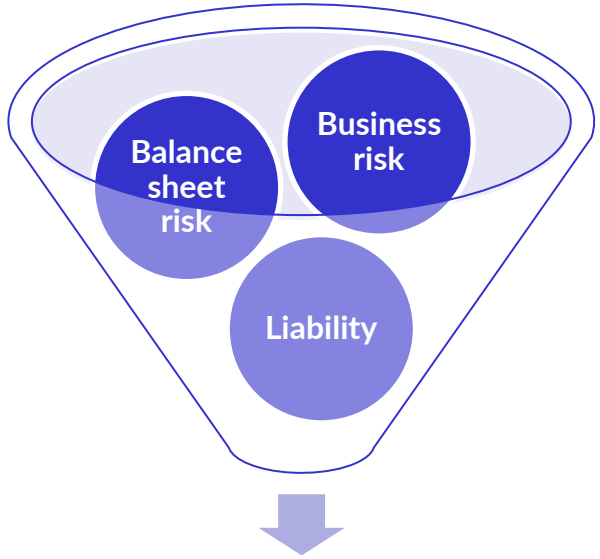
- Offers both services & financial risk transfer.

INCIDENT RESPONSE: To determine what happened, how to repair the damage, to reduce downtime and to meet privacy regulatory requirements. Includes IT Forensics, Legal, PR, notification costs, and restoration costs.

LAWSUITS & PRIVACY REGULATORY INVESTIGATIONS: Legal fees, legal settlements and also regulatory fines where insurable (such as HIPAA, PCI, GDPR, CCPA, etc violations)

CYBER CRIME: Costs such as ransom or extortion payments, phishing, and social engineering.

BUSINESS LOSSES: Impact to operations or ability to generate revenue both during an incident and afterward as it impacts your reputation.



Reputation

1st Party Coverages

- **Incident Management Costs:**
  - Breach / Incident Response Costs (IT Forensics & Legal/Breach Coach)
  - Notification Costs / Credit Monitoring / Call Center
  - Crisis Management / Public Relations

- **Crime Costs**
  - Extortion
  - Funds Transfer Fraud / Computer Fraud – *sometimes the same*
  - Funds Transfer Fraud / Social Engineering – *sometimes the same*
  - Service Fraud / Telecom Fraud

1st Party Coverages

- **Business Interruption & Extra Expense Coverages**
  - Business Interruption
  - Dependent Business Interruption – *IT vs. Non IT Partners*
  - Extra Expense
  - Reputational Harm

- **System Restoration Expenses**
  - Digital Asset Restoration
  - Computer Hardware / Bricking
  - Betterment – *as a % or set limit*

3rd Party Coverages

- **Network Security Liability**
- **Privacy Liability**
- **Regulatory Defense & Penalties**
- **PCI Fines & Penalties**
- **Media Liability**
  - Defamation, IP Infringement, Libel, Slander, Disparagement

COVERAGE CONSIDERATIONS:

- **Adequacy of Limits** – benchmarking
- **Policy Aggregates vs. Limits outside the aggregate**
  - Typically limited to “Breach Response Costs”
- **Retroactive Dates** – *full prior acts*
- **Regulatory Coverage** – *is it broad?*
  - *Evolving Regulations (GDPR, CCPA, Biometric data)*

COVERAGE CONSIDERATIONS

- **Cyber Crime**
  - **Extortion (Ransomware) Limitations** – sublimits, coinsurance, deductibles, aggregates
  - **Social Engineering**
  - **Reverse Social Engineering / Invoice Manipulation Fraud / Push Payment Fraud**
  - **Theft of personal funds of executives** – *not common*
  - **Corporate identity theft** – *not common*

COVERAGE CONSIDERATIONS

- **Business Interruption & Extra Expenses**
  - **Dependent / Contingent Business Interruption** – *check for sublimits*
    - IT Partners vs. Supply Chain Partners
  - **System Failure** – included?
  - **Reputational Harm** - sublimits and period of indemnity
- **System Restoration Expenses**
  - **Computer Hardware Replacement / Bricking**
  - **Betterment**

COVERAGE CONSIDERATIONS

- **Other :**
  - **Bodily Injury**
  - **Property Damage**
  - **Pollution**
  - **Duty to Defend**
  - **Pay on behalf of** or **reimbursement**
  - **Wrongful Collection – biometric data, meta pixels, etc**

COVERAGE CONSIDERATIONS

- **Keep an eye out for:**
  - **Stipulations around breach or ransomware event handling – "discovered"?**
  - **Patching requirements – "neglected software exploitation" exclusion**

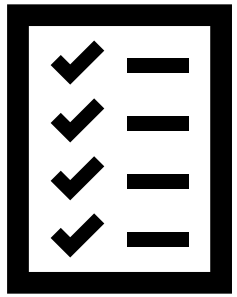
Sub-Limited Coverage Extension for **Neglected Software Exploits**		
Period of Neglect	Coinsurance	Limit of Insurance per **Policy Period**
0 – 45 days	0%	$<LIMIT01>
46 – 90 days	5%	$<LIMIT02>
91 – 180 days	10%	$<LIMIT03>
181 – 365 days	25%	$<LIMIT04>
Longer than 365 days	50%	$<LIMIT05>

COVERAGE CONSIDERATIONS

- **Keep an eye out for:**
  - **Widespread Event Exclusions**
  - **War & Terrorism Exclusion**
    - **Cyber Terrorism – carved back?**
    - **Nationstate Activity Exclusions**
  - **Warranties – your application as a warranty**

Underwriting Criteria / Requirements

- Multi-Factor Authentication
  - Remote, Privileged (incl. Backups), and Email Access
- Secured Remote Connectivity – No Public RDP
- System Updates & Proper/Timely Patching
- Segregated & Secured Backups – tested?
- Employee Training
- Cyber Incident Response Policy – tested?
- Financial Transaction Multi-Authentication/Approval Process
- Intrusion Detections Systems & Endpoint Detection
- Endpoint Detection & Response (EDR)
- NextGen Antivirus
- Data Encryption – at rest, in transit
- Penetration Testing
- Vulnerability Assessment
- Vendor Management
- 24/7 SOC
- Email Security & Filtering
- Privileged Access Management



STATE OF THE MARKET

- **2021 & 2022 Significant Rate Increases**

Ransomware attacks increase by 170%, drive cyber insurance rates

July 07, 2021

Ransomware attacks driving cyber reinsurance rates up 40%

Willis Re International told Reuters that recent high-profile ransomware attacks are sending reinsurance rates soaring.

By Jonathan Greig | July 2, 2021 -- 20:33 GMT (13:33 PDT) | Topic: Security

Global cyber insurance pricing increases 32%: Howden

Luke Harrison 05 July 2021

Cyber industry loss ratio at record-high 67% in 2020: Aon

21st June 2021 - Author: Matt Sheehan

Cyber Insurance Market

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Source: "Report on the Cyber Insurance Market" Memo issued October 18, 2022

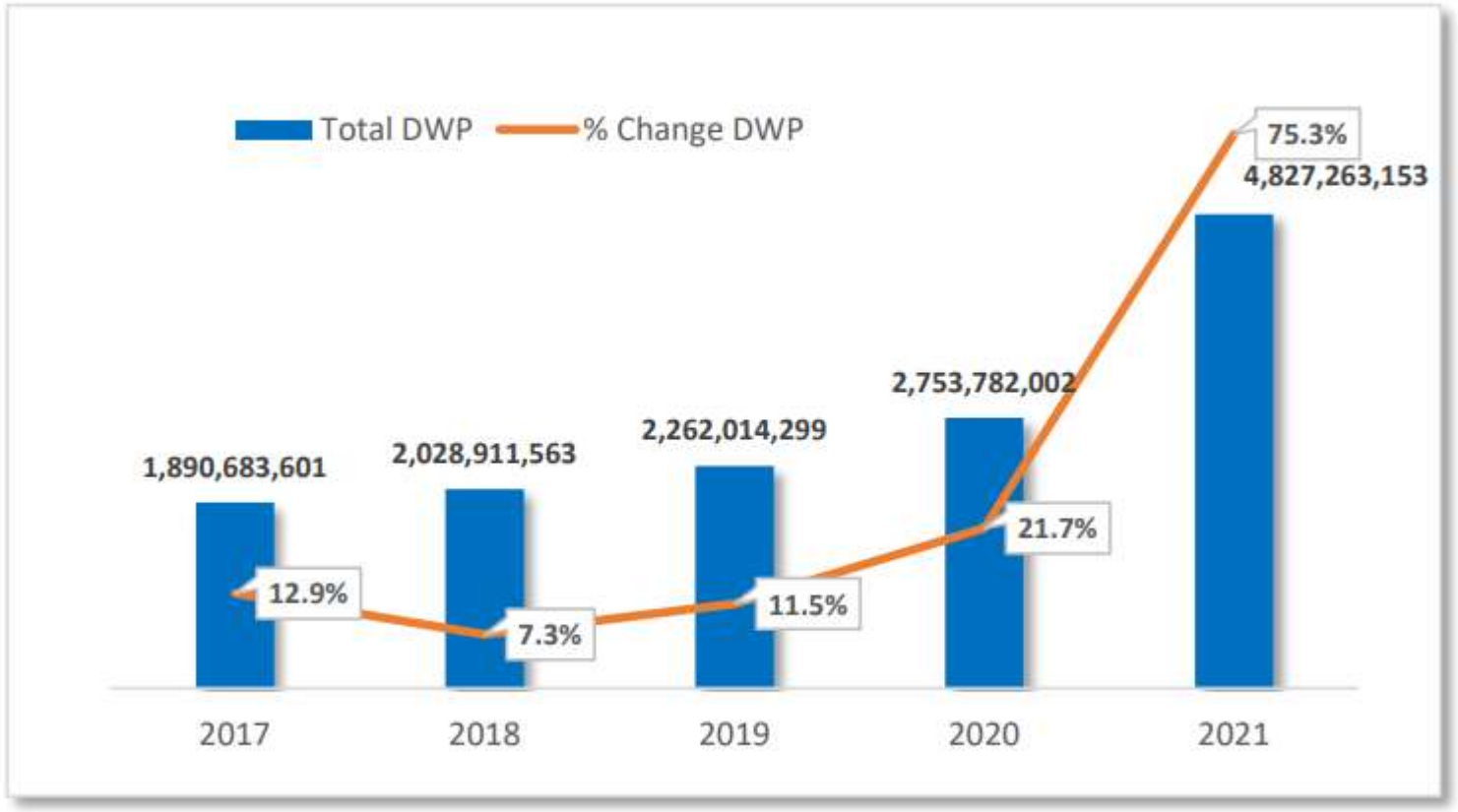
Year	Direct Written Premium Stand-Alone Cyber Policies - U.S. Domiciled Insurers (1)	Direct Written Premium Package Cyber Policies - U.S. Domicilied Insurers (2)	Direct Written Premium Stand-Alone Cyber Policies - Alien Surplus Lines Insurers (3)	Direct Written Premium Package Cyber Policies - Alien Surplus Lines Insurers (4)	Stand-Alone Policy Totals Direct Written Premium (All Insurers) (1+3)	Package Policy Totals Direct Written Premium (All Insurers) (2+4)	Total Direct Written Premium Written (1+2+3+4)
2015	483,197,973	932,645,734	*Not Reported	*Not Reported	483,197,973	932,645,734	1,415,843,707
2016	811,057,406	863,769,169	552,226,000	156,285,000	1,363,283,406	1,020,054,169	2,383,337,575
2017	994,259,551	896,424,050	765,129,000	431,423,000	1,759,388,551	1,327,847,050	3,087,235,601
2018	1,113,865,104	915,046,459	781,260,000	346,380,000	1,895,125,104	1,261,426,459	3,156,551,563
2019	1,263,214,669	998,799,630	890,627,667	204,230,452	2,153,842,336	1,203,030,082	3,356,872,418
2020	1,618,747,678	1,135,034,324	961,228,993	350,117,810	2,579,976,671	1,485,152,134	4,065,128,805
2021	3,151,977,648	1,675,285,505	1,385,498,876	330,414,781	4,537,476,524	2,005,700,286	6,543,176,810

Cyber Insurance Market

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Source: "Report on the Cyber Insurance Market" Memo issued October 18, 2022

Figure 1. Direct Written Premium and Percent Change by Year (Does Not Include Alien Surplus Lines Data)

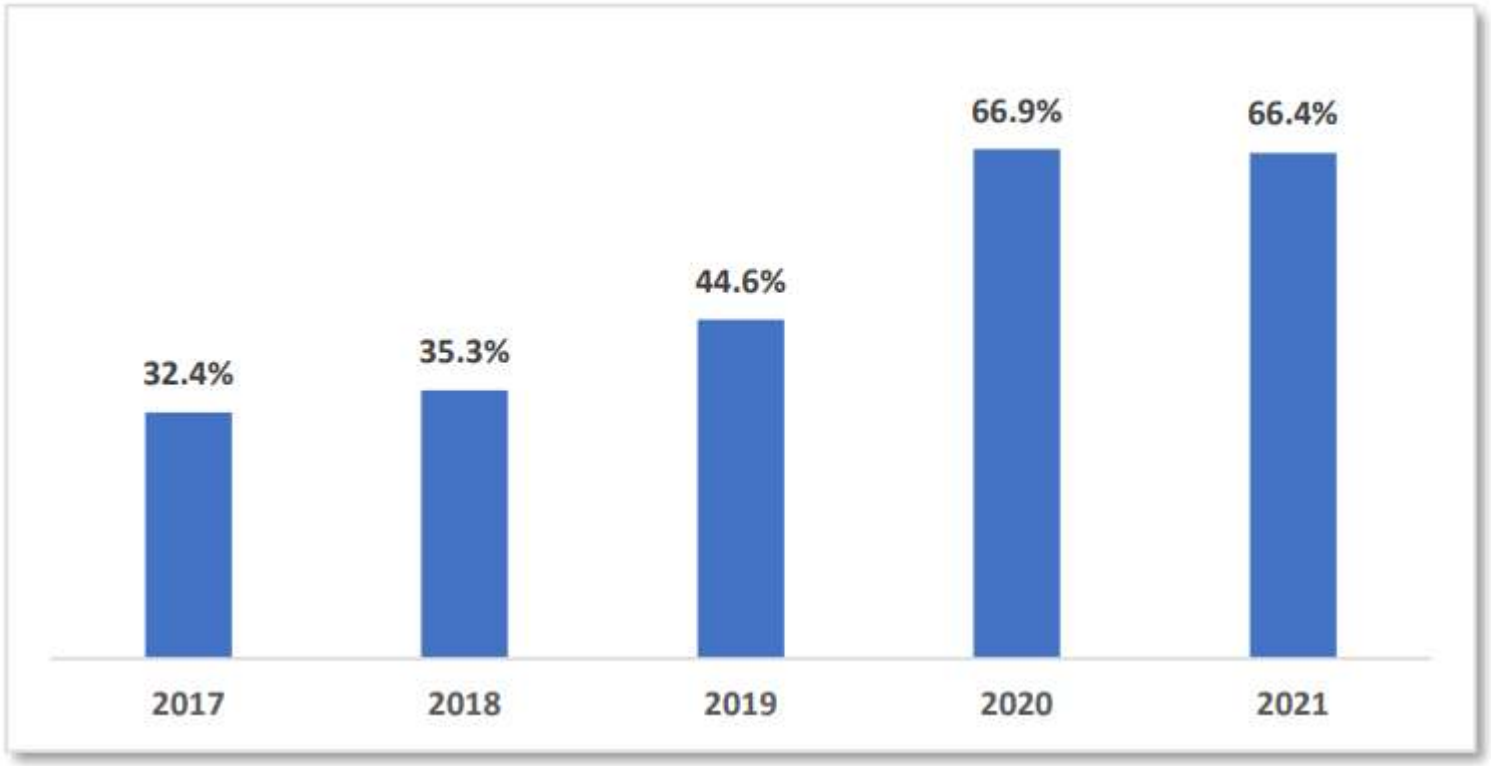


Cyber Insurance Market

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Source: "Report on the Cyber Insurance Market" Memo issued October 18, 2022

Figure 2. Loss Ratios with Defense and Cost Containment (DCC) Stand-Alone and Package Policies Combined (Does Not Include Alien Surplus Lines)



2023 State of the Market

- **Capacity stabilizing**
- **Focus on sustainable pricing and retentions**
- **Coverage changes –** nation state attacks, wrongful collection exclusions
- **Detailed underwriting information & cyber security controls**
- **Keep an eye on regulations –** biometric data & otherwise
- **Trend towards “inside out” underwriting**

REGULATORY ENVIRONMENT

- Ransomware – legality of payment questioned
- Privacy Laws – biometric data, pixel tracking
- Stronger reporting requirements
  - Federal Critical Incident Reporting for Critical Infrastructure Act of 2022
  - Pending clarity on what constitutes a cyber incident and who qualifies as critical infrastructure

North Carolina bans state entities from negotiating with hackers - and other states may follow

March 18, 2022

New Cybersecurity Law Will Require Cyber-Incident Reporting for Critical Infrastructure

Lloyd's Will No Longer Include Nation-State Attacks in its Cyber Insurance Policies

Luke Irwin 25th August 2022

Takeaways

1) Review Cybersecurity Controls/Posture
2) Review Insurance Coverage
3) Incident Response Plan - tabletop

johnson
kendall
johnson

Thank you!

Alexandra H. Bretschneider
abretschneider@jkj.com