AMWINS™

Construction Cyber Risk & Response:

Yesterday, Today and Tomorrow

Presented by:

Craig Dunn & Garet Philbrook

Introduction

Craig Dunn

Executive Vice President, Broker

E-mail: craig.dunn@amwins.com

Phone: 214.561.6872

Garet Philbrook

Assistant Vice President, Broker

E-mail: garet.philbrook@amwins.com

Phone: 832.356.7184

AMWINS®

Gain the Access + Expertise of Amwins Professional Lines Practice

Why Amwins?

Expertise: Our professional lines expertise extends across numerous lines of coverage and classes of business. Through continuous program assessment, placement strategy and form review, we deliver custom solutions that meet your clients' unique needs.

Collaboration: Our professional lines specialists constantly collaborate across teams, geographies and divisions. When you work with an Amwins professional lines broker, you get the knowledge and expertise of our entire firm.

Proprietary products: We offer numerous proprietary professional lines products tailored to specific classes and lines of business. We also leverage a variety of portals and pre-negotiated terms to help us transact more efficiently on your behalf.

Areas of Specialty

Our professional lines specialists harness their expertise in various coverage lines to deliver tailored insurance solutions.

Our core product strengths include, but are not limited to:

Cyber Liability

D&O
- Private
- Public
- Non-profit

E&O
- Technology
- Real estate
- Misc. professional liability

Employment Practices Liability
- Wage & hour

Healthcare
- Medical professional
- Long-term care

Licensed professionals
- Architects & engineers
- Contractors
- Lawyers

Financial Institutions and Financial Service Firms
- Asset manager
- Hedge funds
- Investment advisers
- Private equity
- Mutual funds
- Family offices
- REITs

Public Entity
- Educator's legal liability

Our Divisions

We're structured to deliver products and services that meet your client's unique needs

AMWINS™

AMWINS™ BROKERAGE

Amwins brokers have expertise in placing property, casualty and professional lines coverage for complex and unique risks.

AMWINS™ ACCESS

Amwins Access is a nationwide binding platform for small commercial and personal lines business, targeting accounts less than $10,000 in premium.

AMWINS™ UNDERWRITING

Comprised of industry specialists, Amwins Underwriting delivers unmatched underwriting acumen and results to our partners.

AMWINS™ GROUP BENEFITS

Amwins Group Benefits is a General Agent, TPA, MGU and Benefit Service provider uniquely focused on being your one-stop expert.

AMWINS™ INTERNATIONAL

Amwins Global Risks, formerly THB, serves clients in over 150 countries to place specialty insurance and reinsurance coverage.

Brokerage Division

Areas of specialty span a wide range of coverage for challenging, complex or emerging risks, including but not limited to:

Property

- Wind/Quake/Flood
- Builder's Risk
- Inland Marine
- Exclusive Facilities

Casualty

- Umbrella/Excess Liability
- Commercial General Liability
- Products Liability/Product Recall
- Auto Liability
- Workers' Compensation

Professional Lines

- Cyber
- D&O: Private, Public, Non-profit
- E&O
- Employment Practices
- Financial Institutions

Alternative Risk

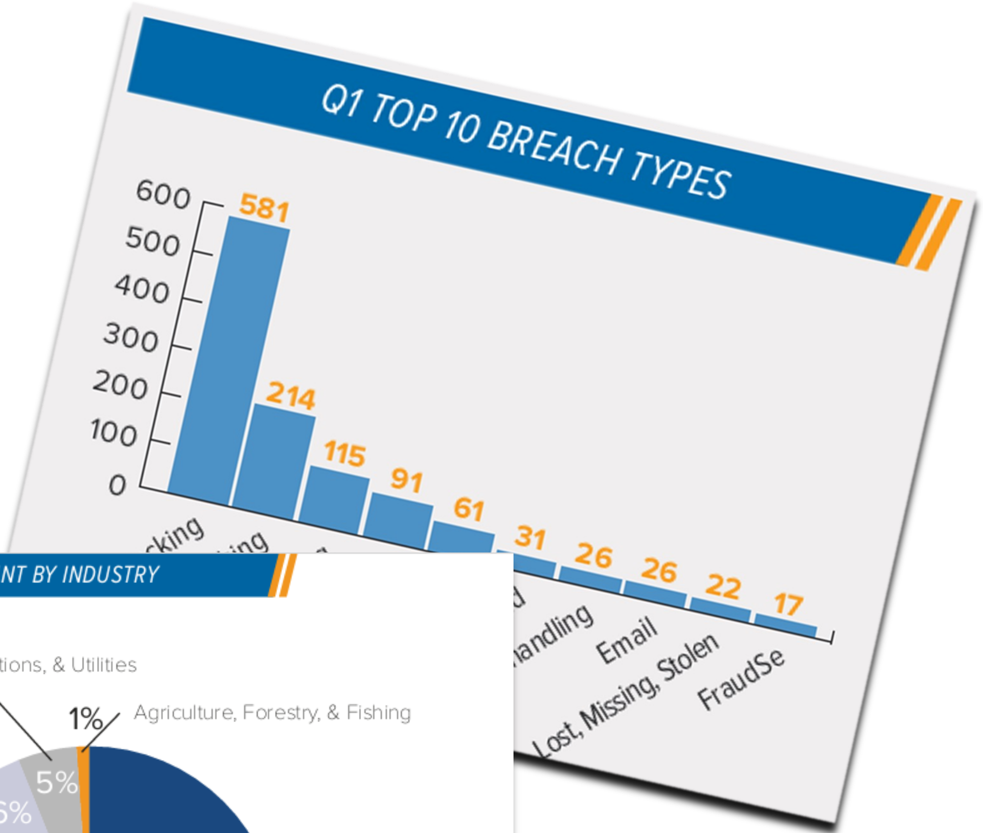
- Parametric structures
- Captives
- Reinsurance
- Bermuda market expertise

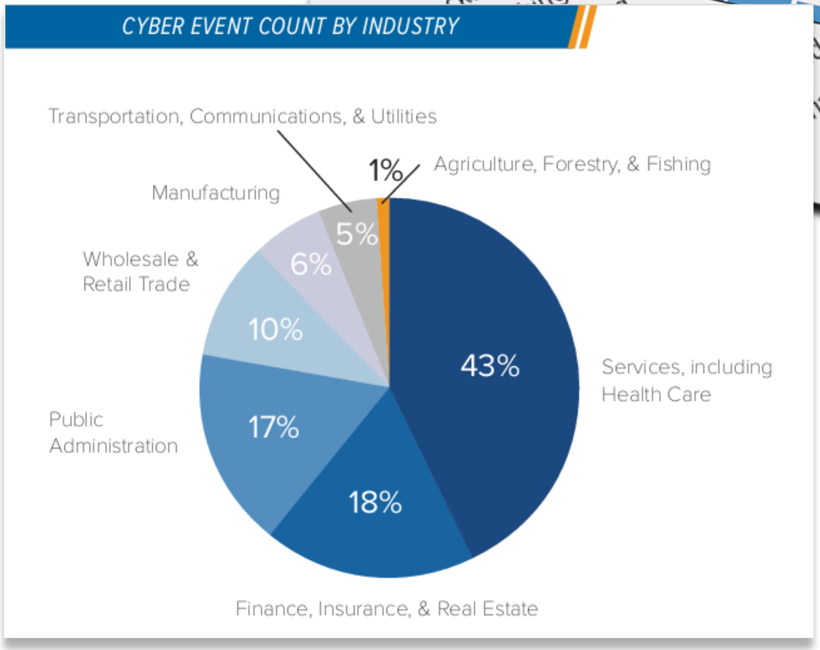
Evolution of Cyber Risk

Continually evolving Exposure

- Motivated attackers +
- Effective tools +
- High potential for loss +

= RISK





Cyber Risk

… Follows the **money**

Early years…

Focus on personal data (health, credit card, and private)

Targeted fraud schemes (phishing, social engineering, invoice manipulation)

Resource fraud

Today…

Interruption in business activities. Financial to physical form of loss.

On the horizon…

Hacktivism & politically motivated attacks

History & Development of Cyber Coverage

Cyber Insurance Coverage

… Follows the **risk**

RISK	COVERAGE
Early years… Focus on personal data (health, credit card, and private)	Third party only
Targeted fraud schemes (phishing, social engineering, invoice manipulation)	First Party / traditional Crime Coverages
Resource fraud	Supplemental sublimits/ enhancements
Today… Interruption in business activities. Financial to physical form of loss.	Business Interruption “Bricking” Contingent Bodily Injury Prevalence of “Silent Cyber”
On the horizon… Hacktivism & politically motivated attacks	Cyber Terrorism Collaboration with government & private security sector

Continually evolving…

- 70+ Carriers with stand-alone cyber forms (est.)
- Over 200 carriers provide some form of cyber cover – either on a package basis or blended forms (est.)
- Annual updates to stay relevant
- Limited standardization among forms/ carriers

13 Key Insuring Agreements	
Coverage Type	**Insuring Agreement**
First-Party/Post-Breach Response Coverage	1. Privacy notification and crisis management expense
Third-Party/Liability Coverages	2. Information security and privacy liability 3. Regulatory defense and penalties 4. Payment card industry fines and assessments 5. Website media 6. Bodily injury (BI) and property damage (PD) liability
First-Party/Time-Element Coverages	7. Business interruption 8. Extra expense
First-Party/Direct Property Loss Coverages	9. Data assets 10. Cyber extortion 11. Computer fraud 12. Funds transfer fraud 13. Social engineering coverage

- Cyber liability insuring agreements (Source: IRMI)

- Increasing Premiums
- Limiting Coverage
- Stricter Security Requirements
- Non-Renewing Industries
- Carriers Exiting

Current State of the Market

Cyber Insurance

Cyber: State of the Insurance Market

01 Decreasing capacity

But there is still capacity, and underwriters do have appetite for new risks.

02 Increasing Rates

Expected to continue through 2022 to 2024

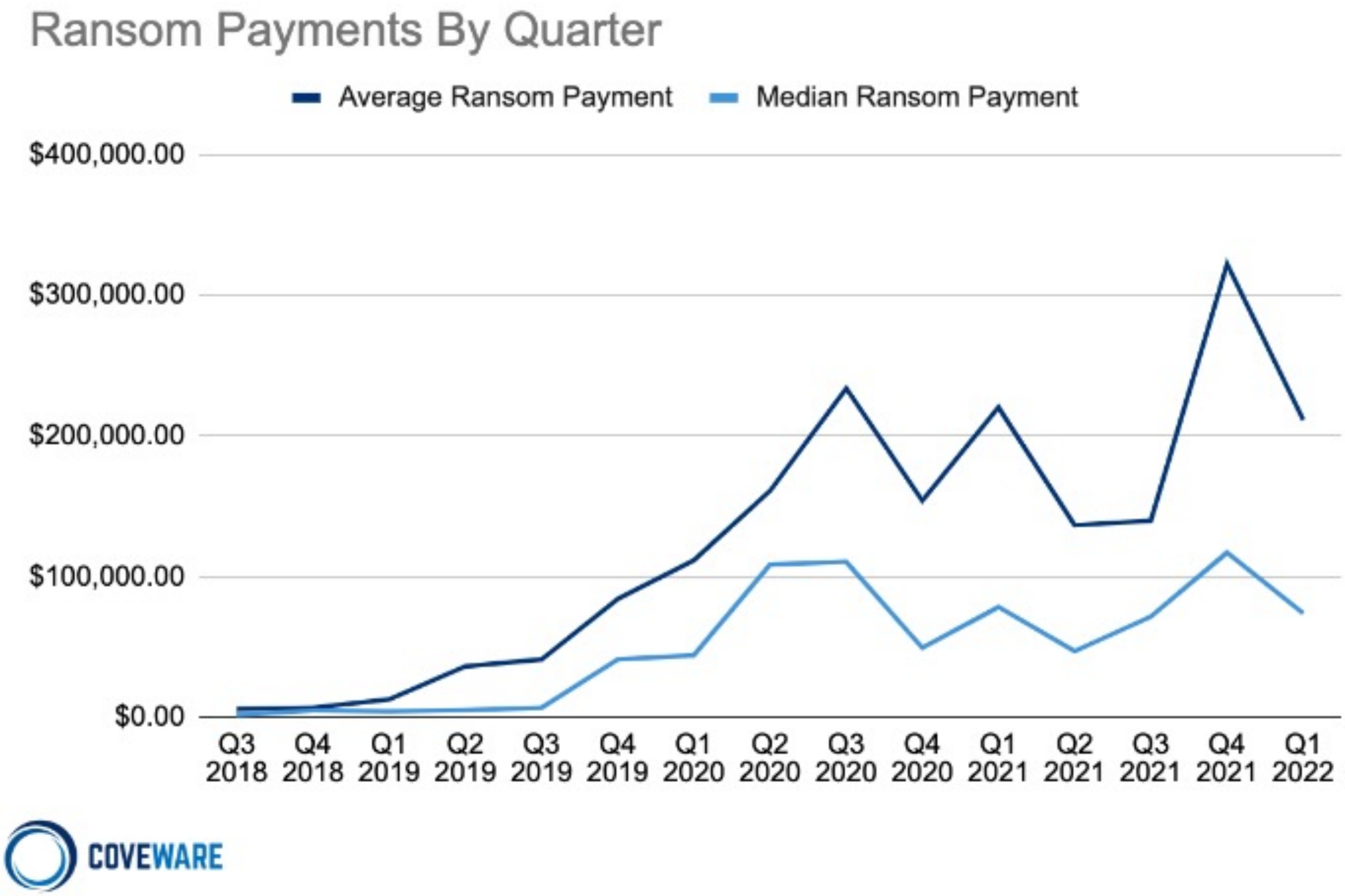
03 Onus on Insureds for minimum / base controls

Including: implementation of MFA; Secure RDP's; robust backup procedures and Incident Response Plans

04 Prevalence of "Silent" Cyber

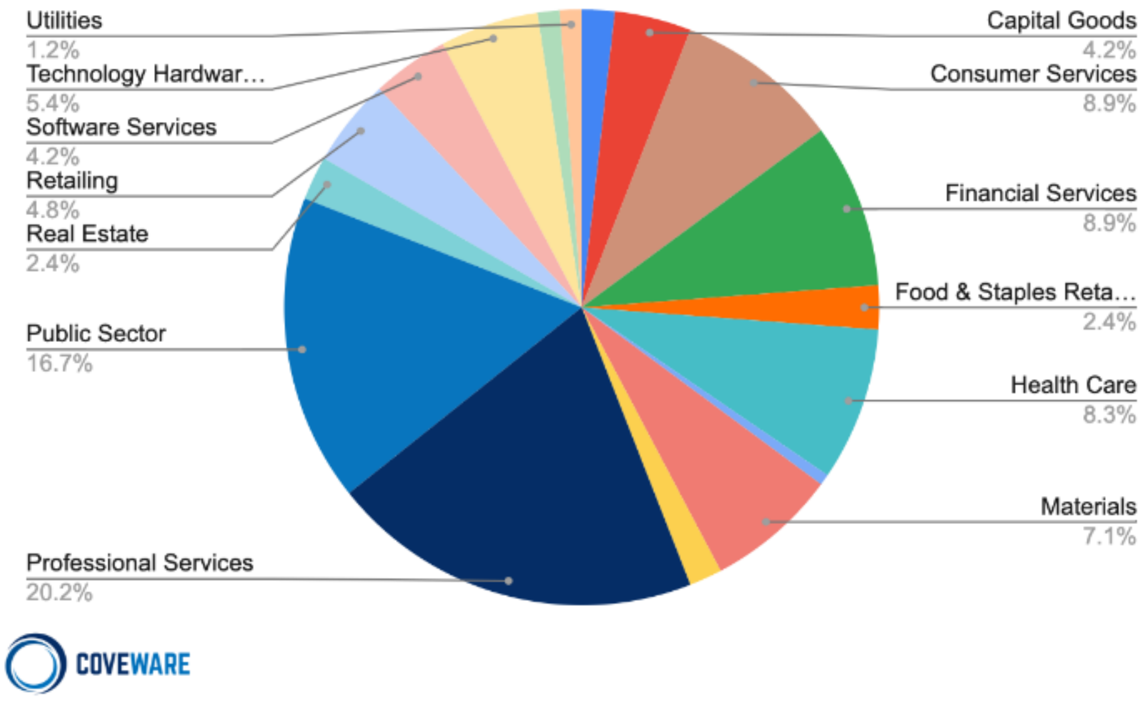
Gaps in coverage programs can occur as a result of cyber risk.

Ransomware Spotlight

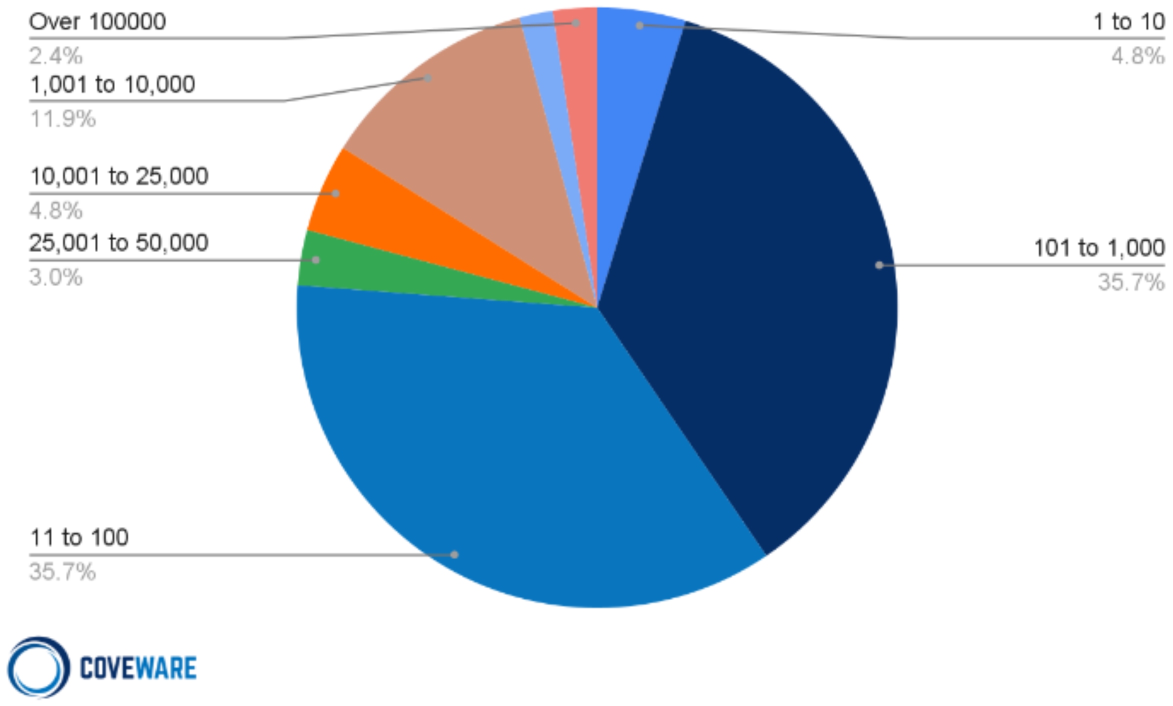

Ransom Payments By Quarter
Average Ransom Payment
Median Ransom Payment
$400,000.00
$300,000.00
$200,000.00
$100,000.00
$0.00
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
Q3 2020
Q4 2020
Q1 2021
Q2 2021
Q3 2021
Q4 2021
Q1 2022
COVEWARE

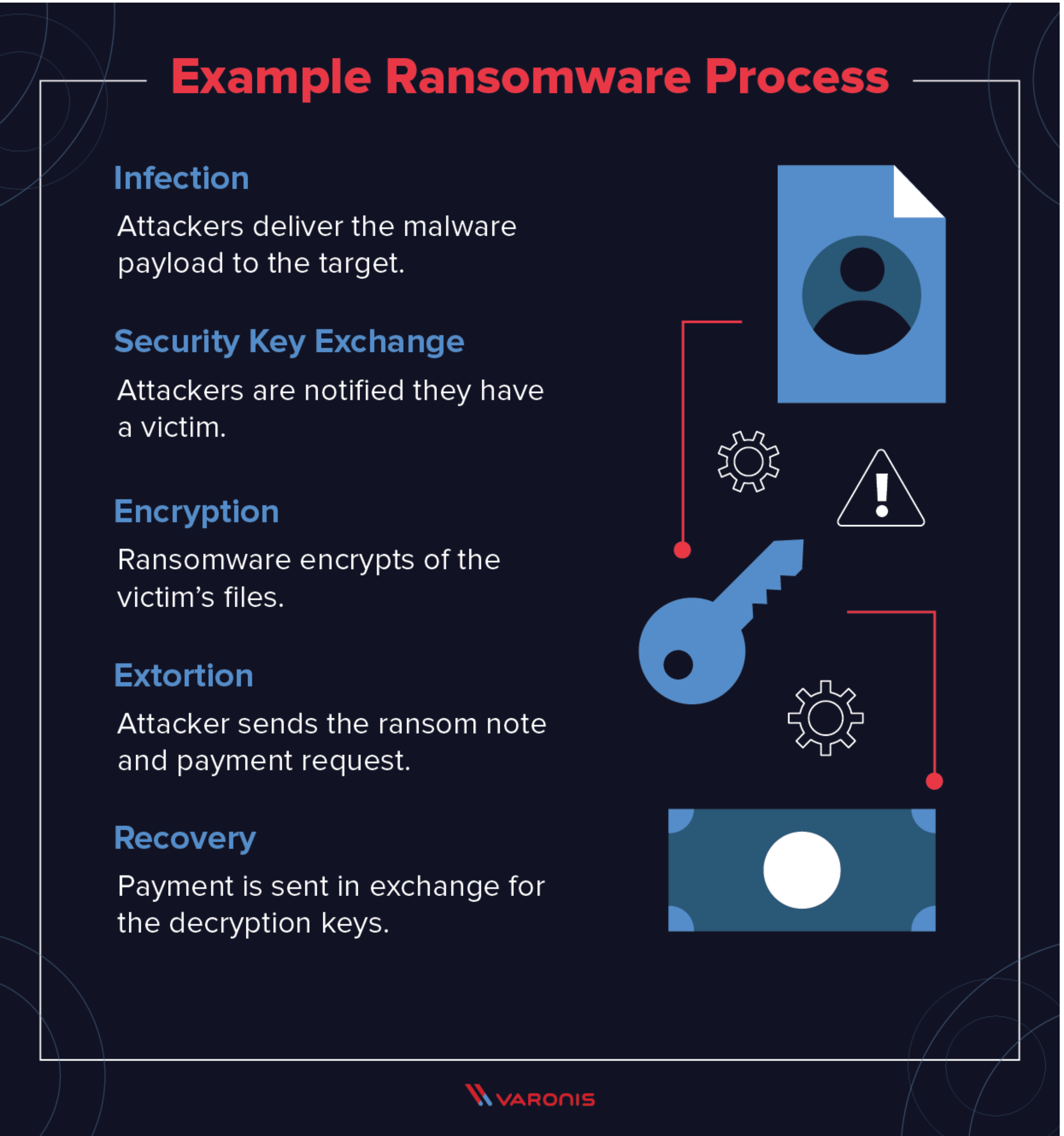
Ransomware Targets

Industry



Size





RANSOMWARE:

A combination of "**RANSOM**" and "soft**WARE**"

- It is not a virus, but a different form of "Malware"
- Most typically it is installed via someone clicking a malicious link or downloading a malicious file.

2 major types:

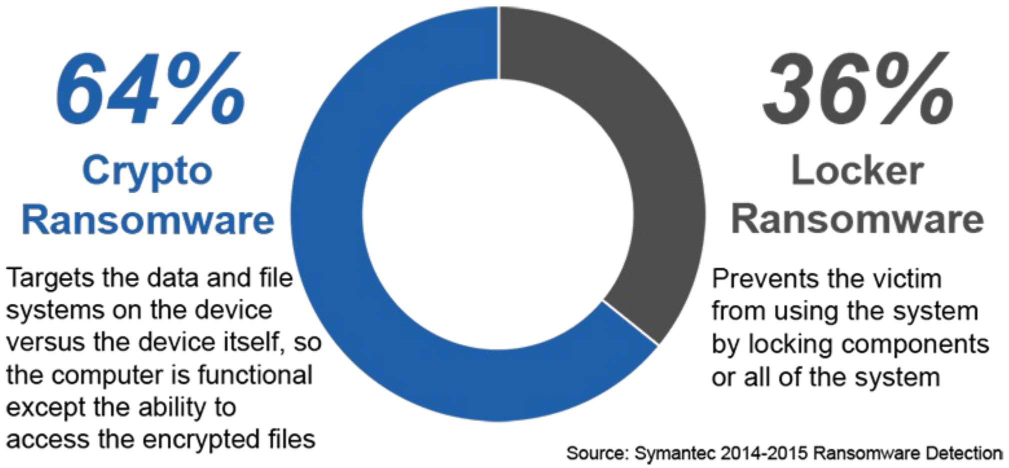


Image Source: Varonis Blog

EVOLUTION:

- **Early 2000's**: few individuals had the ability and to be "dangerous". Hacking for sport. First known variants emerged in 2005

- **Since that time**: Companies and targeted organizations began to adapt and shore up defenses.

  - 2009 saw the genesis of file encryption methods
  - 2010 saw the birth of Bitcoin which increased monetization
  - 2014 saw emergence of over **250k** ransomware samples
  - 2015 saw over **4 million** ransomware samples

- **Where are we today?**
  - Ransomware as a service (RaaS)
  - Nation state attacks
  - Big game hunting

Source: https://www.crowdstrike.com/wp-content/uploads/2019/05/evolution-of-ransomware-from-2005-2019.png

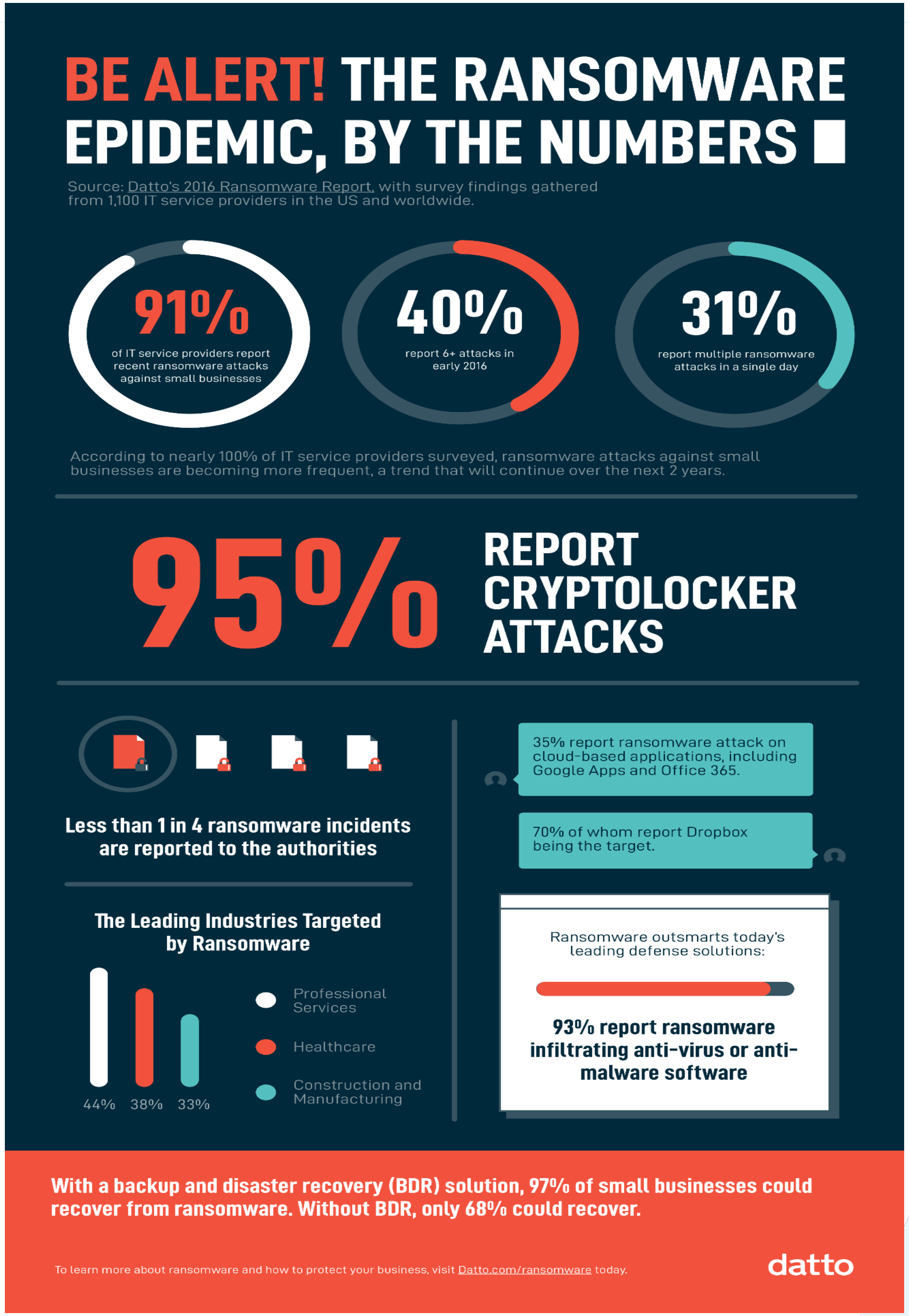
Construction At-Risk?

- **Ransomware does not discriminate:**
  - Hackers are looking for “low hanging fruit”
  - Any company connected to the internet is at risk.
  - Cost to deploy Ransomware attacks are low, and effort is minimal, so any monetary return is considered a bonus on those less sophisticated attacks

- **Connectivity is paramount:**
  - Hackers understand how dependent our society is on being “connected”
  - Businesses are now more depending on internet connectivity to operate and make money, so when that access is taken away, it’s very problematic
  - With an internet connection, companies have “end-points”… essentially where the network ends…Any endpoint is a potential vulnerability

According to a SANS Institute study, 53% of organizations’ endpoints have been compromised at some point.

And - Ransomware can enter through the endpoint or can be triggered there

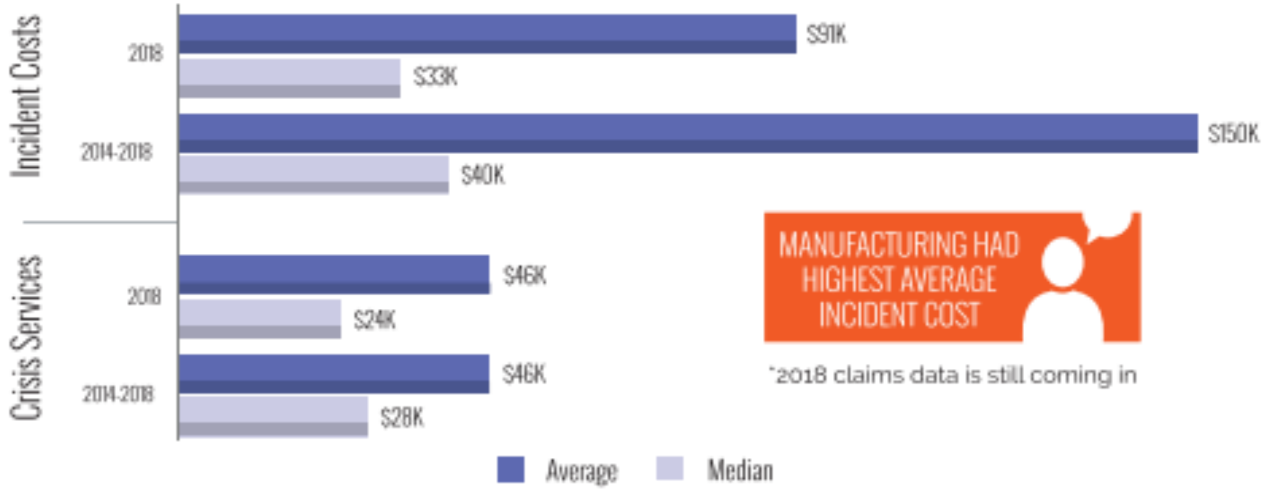


What's the risk?

- Crippling costs
- Ransom amounts are climbing
  - According to NetDiligence Claims study in 2020, the average ransom amount in 2018 was $72k
  - More now…
- Associated Costs are increasing
  - Loss isn't limited to the ransom amount. Costs incurred to employ an incident response team and deal with the related costs to mitigate the damage are very high
- Effects of Business Interruption are worsening
  - As more businesses rely on internet connectivity to operate, the downtime is particularly impactful

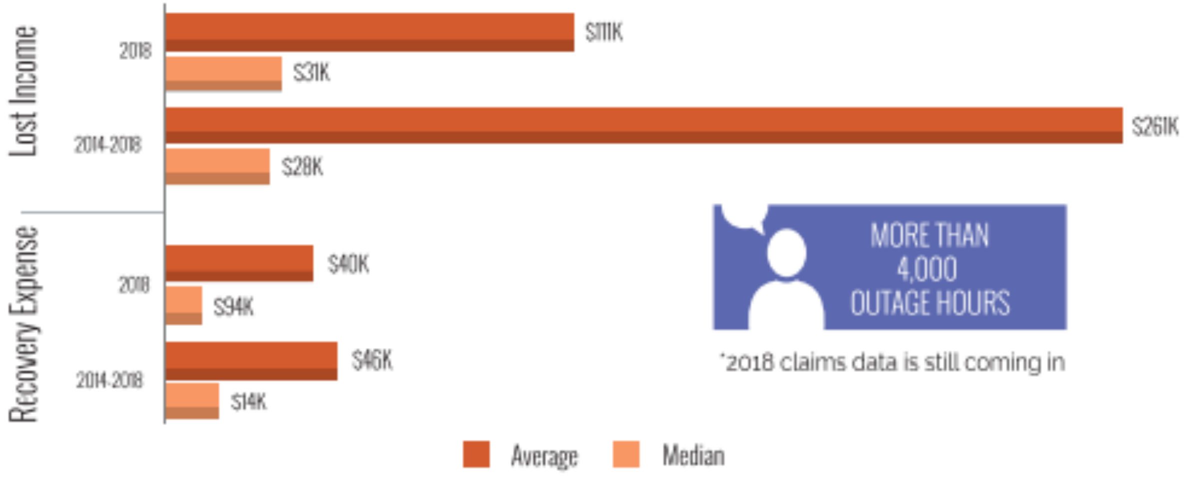
Source: NetDiligence Ransomware study 2020

Costs are increasing*

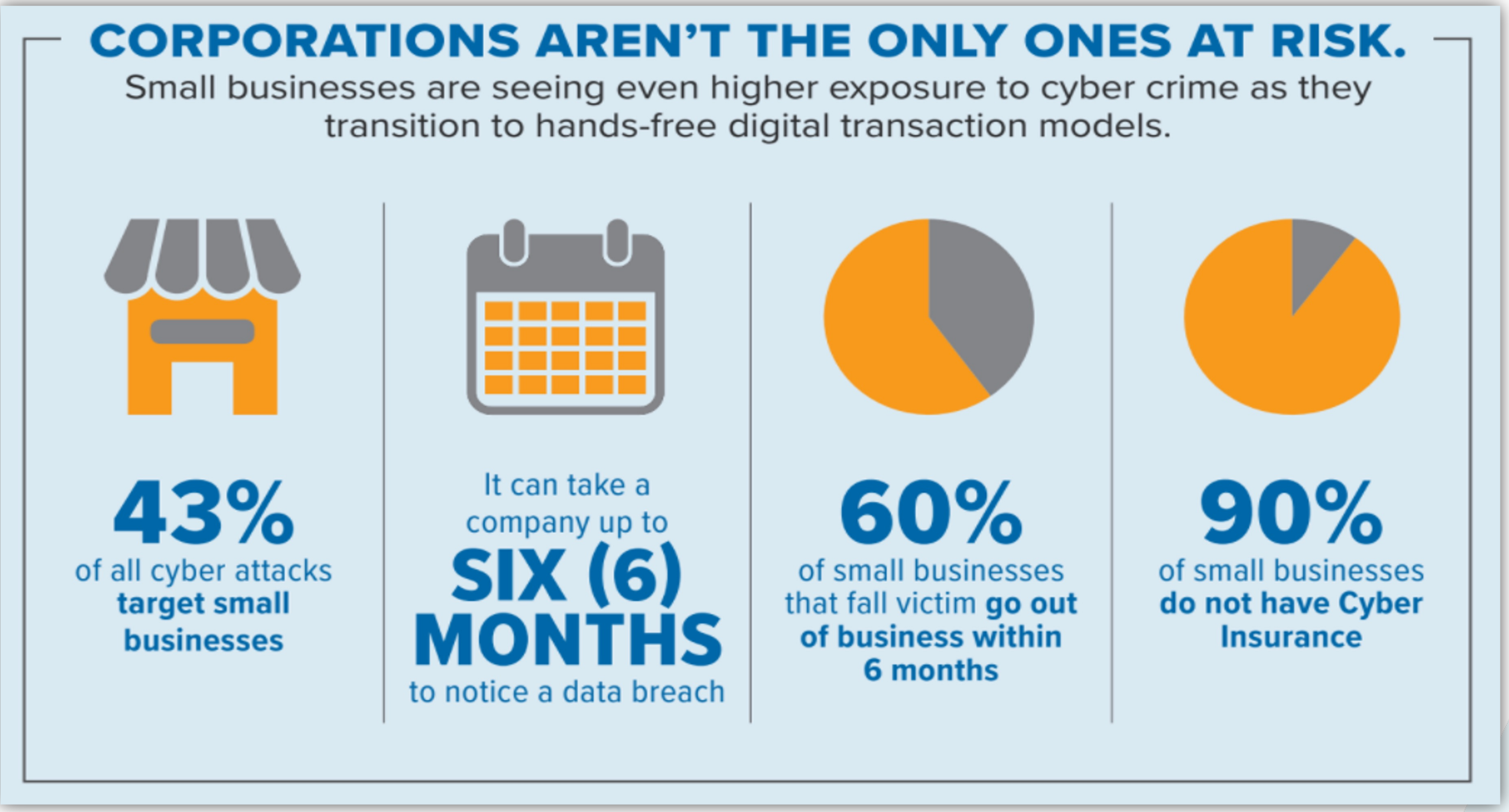


Total Incident and Crisis Costs

Effects of business interruption are worsening*



Lost Income and Recovery Costs


CORPORATIONS AREN'T THE ONLY ONES AT RISK.
Small businesses are seeing even higher exposure to cyber crime as they transition to hands-free digital transaction models.
43%
of all cyber attacks target small businesses
It can take a company up to
SIX (6) MONTHS
to notice a data breach
60%
of small businesses that fall victim go out of business within 6 months
90%
of small businesses do not have Cyber Insurance

Claims Examples & Case Studies

Social Engineering, Ransomware, and Outdated Software

Cyber Case Study:
Social Engineering

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	$8,625
Legal fees	$6,570
FUNDS TRANSFER FRAUD Transferred funds not recovered	$31,400
TOTAL POTENTIAL CLAIM	$46,595

Situation:

A slate installation contractor's emails were accessed by an attacker who, posing as the General Manager, asked an employee to contact the broker's bank with instructions for funds to be transferred into the hacker's bank account. When the contractor discovered that unauthorized payments were made totaling $270,000, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $238,600 of the unauthorized transactions.

Resolution:

The contractor has a stand-alone cyber policy that covers social engineering as well as provides crucial response services. Once the contractor notified their insurance company, an IT forensic consultant was appointed to assist the contractor in repairing the damage to their system as well as to prevent future attacks. As the contractor has expanded cyber crime coverage under their policy, they were reimbursed for the direct financial loss, less the deductible, of the unrecovered fraudulent transfers as well as their forensic and legal costs.

Credit: Sayata Labs

Cyber Case Study:
Ransomware

Total estimated cost for ABC Insurance Brokers

Total cyber loss estimates may be great as this calculation does not include: regulatory fines, penalties, PCI-DSS assessment expenses, cyber crime/ financial fraud, and reputational loss

Over 15 days	Over 30 days	Over 60 days
$627,739	$655,479	$710,958

Situation:

ABC Insurance Brokers suffered a ransomware attack after an employee opened a phishing email attachment which encrypted all of its systems and workspaces.

Resolution:

After reporting the claim to the carrier, ABC was introduced to recommended privacy counsel and a forensics firm. While the threat actor did not respond to contact and so no ransom could be paid, with the assistance of Corvus-approved IT vendors, the policyholder successfully restored all data. Costs incurred included legal, forensics, and data recovery.

Credit: Corvus Insurance

Cyber Case Study: Outdated Software

POTENTIAL IMPACT	
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$24,470
Identity theft and credit monitoring services	$13,860
Incident response fees	$16,050
Public relations fees to minimize reputational impact	$18,500
Call center set up and operation to field inquiries	$15,400
NOTIFICATION COSTS	$1,800
DATA RECOVERY Costs associated with replacing lost or corrupted data	$22,850
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	$54,700
Legal expenses and settlement costs for claims	$193,080
Business interruption	$210,815
TOTAL POTENTIAL CLAIM	$571,525

Situation:

Hackers penetrated a residential construction company's network from a vulnerability in an outdated software application. 750 name, address, phone and credit card information were compromised. Local authorities received multiple complaints of suspicious activity, leading the company’s IT department to discover an unauthorized user had accessed the system. Once discovered, the company called their insurance carrier who immediately brought in forensic experts to initiate the company’s IT recovery plan and notification program

Resolution:

The construction company’s cyber policy was triggered, giving them immediate access to response services. The insurance company dispatched a forensic team who quickly isolated the unauthorized user. A claim was started immediately to help with impending legal, consulting and media costs. The insurance company, IT team and forensic consultants ensured the construction company had up-to-date cyber defenses including firewalls, intrusion detection software, and encrypted databases. Concurrently, officials worked with local media to notify affected customers and offer credit monitoring services, while the legal team handled the backlash from those affected. Finally, the forensic consultants helped develop a new plan that included regular updates, testing, and education of all staff to minimize future breaches.

Credit: Sayata Labs & Corvus Insurance

Action Items & Best Practices

Cyber Security Best Practices: Preparation & Preparedness

01 **Multi-factor Authentication (MFA)**

Most effective tool to thwart ransomware.

02 **Robust Backup Procedures**

Off-site, segregated, and up-to-date.

03 **Network Segmentation**

All users do not need access to all data.

04 **Endpoint Detection and Response (EDR)**

Continuously monitor "endpoints" to mitigate threats

05 **Encryption**

Secure the data – at-rest and in transit

06 **Incident Response Plan**

Develop & test.

07 **Employee Trainings**

Phishing simulations, etc.

08 **Patch Management & Security Updates**

Timely deployment of software updates

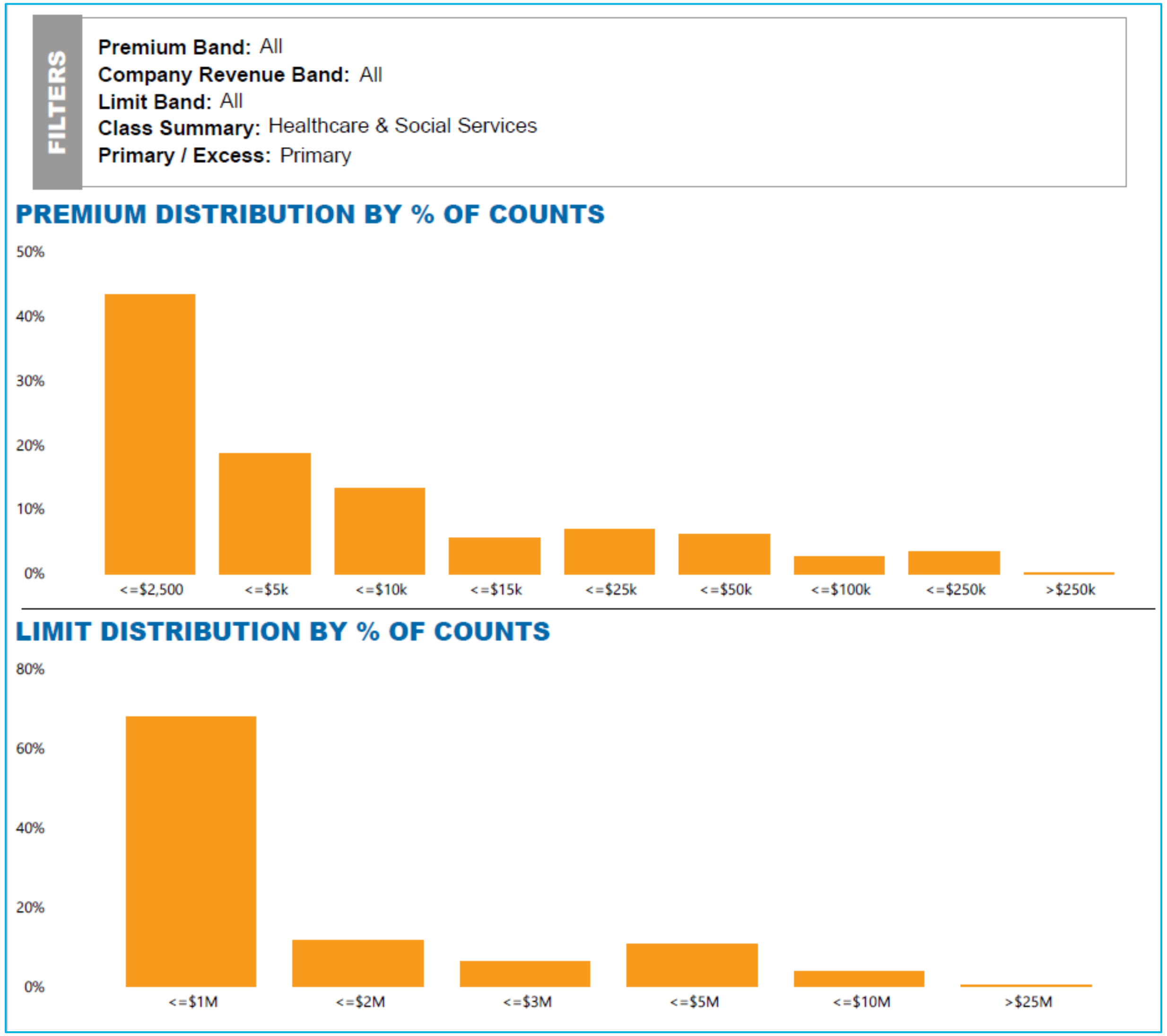
Amwins Capabilities

Cyber

Benchmarking

Proprietary cyber benchmarking tool

- Assists in making policy limit purchasing decisions by analyzing data from thousands of cyber liability placements made by Amwins brokers
- Helps determine what limit and premium are reasonable relative to peer companies within a similar industry and revenue size.
- Can also supplement with Advisen's Cyber OverVue

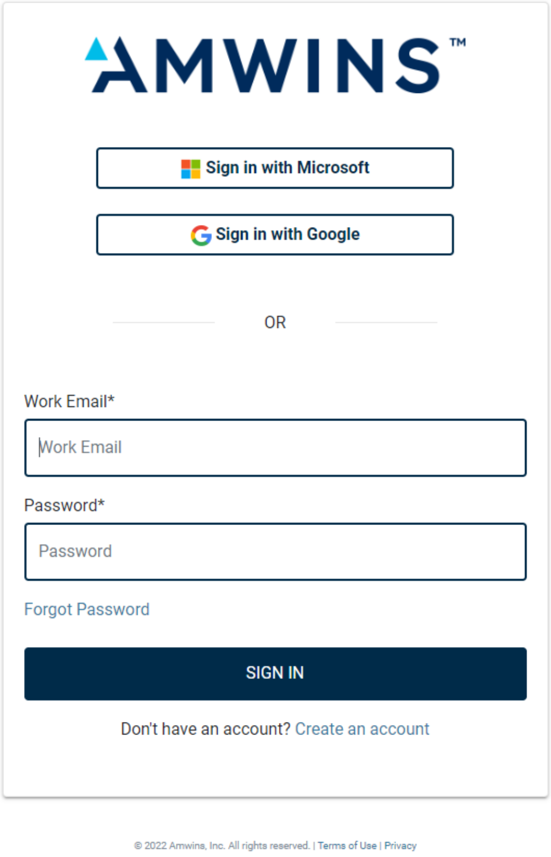


Comparisons & Coverage Audits

	Carrier #2		Carrier #3	
Annual Aggregate?	Annual Aggregate		1st party: Reloadable throughout the Year 3rd party: Annual Aggregate	
Incident Response				
Inside or Outside the Limit?	Outside		Outside	
Forensic IT	$1,000,000	$2,500	$1,000,000	$2,500
Legal	$1,000,000	$2,500	$1,000,000	$2,500
Public Relations	$1,000,000	$2,500	$1,000,000	$2,500
Notification/Credit Monitoring	$1,000,000	$2,500	$1,000,000	$2,500
Ransomware Coverage				
Data and System Restoration/Recreation	$1,000,000	$2,500	$1,000,000	$2,500
Extortion/Ransom Payment	$1,000,000	$2,500	$1,000,000	$2,500
Business Interruption (Cyber Event)	$1,000,000	$2,500	$1,000,000	$2,500
Dependent Business Interruption (Cyber Event)	$1,000,000	$2,500	$1,000,000	$2,500
Business Interruption (System Failure)	$1,000,000	$2,500	$1,000,000	$2,500
Dependent Business Interruption (System Failure)	$1,000,000	$2,500	$1,000,000	$2,500
Reputational Harm	$1,000,000	$2,500	$1,000,000	$2,500
Forensic Accountant	Not Included		$25,000	$2,500
Hardware Replacement Costs	$500,000	$2,500	$1,000,000	$2,500
Cyber Crime Coverage				
Funds Transfer Fraud (Bank Transfers)	$250,000	$12,500	$250,000	$2,500
Computer Crime (Hacker Transfers)	Not Included		$250,000	$2,500
Social Engineering (Employee Transfers)	$250,000	$12,500	$250,000	$2,500
Theft of Personal Funds	Not Included		$250,000	$2,500
Corporate Identity Theft	Not Included		$250,000	$2,500
Service Fraud (Telephone)	$100,000	$2,500	$250,000	$2,500
Service Fraud (Computer)	$100,000	$2,500	$250,000	$2,500
Invoice Manipulation/3rd Party Social Engineering	Not Included		$50,000	$2,500
Liability Coverage				
Privacy Liability	$1,000,000	$2,500	$1,000,000	$2,500
Network Security Liability	$1,000,000	$2,500	$1,000,000	$2,500
Regulatory Fines	$1,000,000	$2,500	$1,000,000	$2,500
PCI Liability & Fines	$1,000,000	$2,500	$1,000,000	$2,500
Media Liability	$1,000,000	$2,500	$1,000,000	$2,500
Management Liability	Not Included		$1,000,000	$2,500
Bodily Injury Liability	Not Included		$250,000	$2,500
Other				
Court Attendance Costs	$25,000	$2,500	$100,000	$2,500
Criminal Reward Coverage	$25,000	$0	Not Included	
Betterment/Post-Breach Remediation	Not Included		$50,000	$2,500
Total Payable				

Professional Lines Portal

Speed and Simplicity



Who's it for?

– Small and middle-market businesses with up to $100M in revenue.

– Available to businesses in every state and most industries.

– Not sure if your risk fits the portal appetite? No problem! We address prohibited classes early in the process

How does it work?

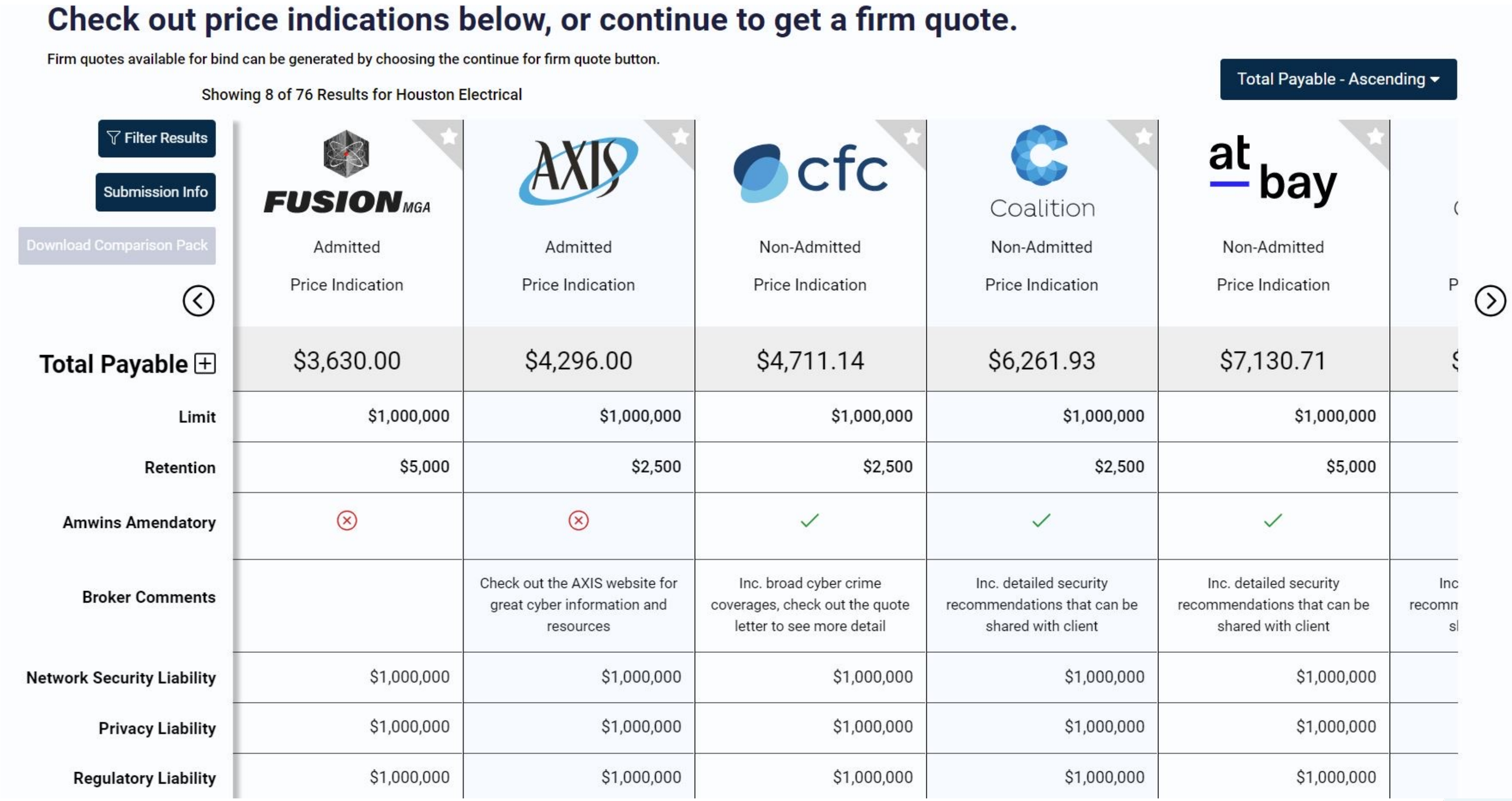
– Amwins' retail partners log-in to our portal at digital.amwins.com and complete one unified set of questions

– You receive instant quotes with limit and retention options from multiple carriers

Amwins Professional Lines Portal

AMPLOP!

- Quick indications or firm quotes
- 3-page master application
- 8 carriers



Check out price indications below, or continue to get a firm quote.

Firm quotes available for bind can be generated by choosing the continue for firm quote button.

Showing 8 of 76 Results for Houston Electrical

Total Payable - Ascending

Filter Results

Submission Info

Download Comparison Pack

	FUSION MGA	AXIS	cfc	Coalition	at bay
	Admitted	Admitted	Non-Admitted	Non-Admitted	Non-Admitted
	Price Indication	Price Indication	Price Indication	Price Indication	Price Indication
Total Payable	$3,630.00	$4,296.00	$4,711.14	$6,261.93	$7,130.71
Limit	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000
Retention	$5,000	$2,500	$2,500	$2,500	$5,000
Amwins Amendatory	⊗	⊗	✓	✓	✓
Broker Comments		Check out the AXIS website for great cyber information and resources	Inc. broad cyber crime coverages, check out the quote letter to see more detail	Inc. detailed security recommendations that can be shared with client	Inc. detailed security recommendations that can be shared with client
Network Security Liability	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000
Privacy Liability	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000
Regulatory Liability	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000

AMWINS™

Any questions?

Craig Dunn

Executive Vice President

214.561.6872

Craig.Dunn@amwins.com

Garet Philbrook, **CPCU, CPLP, RPLU**

Assistant Vice President

832.356.7184

Garet.Philbrook@amwins.com

Thank You!