

The Evolving Cyber Landscape: Threats, Claims, and Technology

June 17, 2020



**Worldwide
Facilities[®], LLC**

Presenter Info

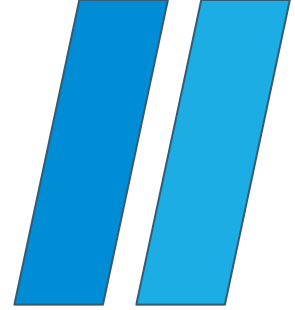


Matt Donovan, RPLU

Worldwide Facilities | Senior Vice President

Matt Donovan graduated from the University of Georgia with a degree in Risk Management and Insurance. He started his career underwriting E&O, Technology & Cyber at ACE Westchester (now Chubb). In 2010 Matt joined Hiscox, a Lloyds of London syndicate, to start their Tech & Cyber practice for the Southeast region. In 2012, he was promoted to Cyber & Technology Product Head & Global Practice Leader. After 10 years of underwriting, Matt joined Worldwide Facilities (a wholesale insurance brokerage) to focus on Cyber & E&O lines of business. He can be reached at (678) 502-1278 or by emailing mdonovan@wwfi.com

Presenter Info



Michael Drummond

At-Bay | Tech & Cyber Product Head

Michael Drummond currently serves as Cyber & Technology Product Head for At-Bay – an insurtech company that helps businesses navigate risk across their technology stack with continuous vulnerability monitoring and security alerts. In this role, Michael is responsible for national product strategy and underwriting management for the company’s cyber and technology insurance portfolio. Michael can be reached via email at michael@at-bay.com

Overview



- The cyber landscape continues to evolve, largely driven by various claims trends that have pushed rapid evolution across the marketplace.
- The early days of nearly exclusive concern over notification expenses following a breach have come and gone, with a new era of business continuity and funds transfer fraud claims driving significant frequency.



Cyber Claims Trends

The cyber threat is real

- Cyber criminals are exploiting phishing schemes and technology vulnerabilities at an unprecedented rate
- Ransomware and financial fraud continue to be the most frequent events and severity of loss is rapidly increasing
- No company or industry is immune - cyber events are affecting companies of all shapes and sizes

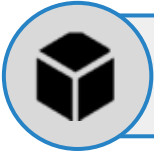
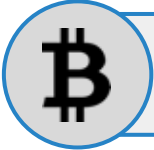
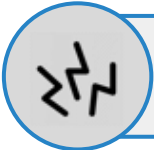


Photo by Michael Geiger on Unsplash

Ransomware continues to evolve



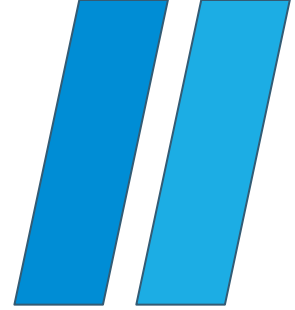
Ransomware has become increasingly more sophisticated and lucrative over time

	<u>Yesterday: Generic</u>	<u>Today: Targeted</u>
 Assets Attacked	Endpoints	Entire networks Backup infrastructure
 Ransom Demand	≤ \$1,000	> \$150,000+
 Damages Incurred	<ul style="list-style-type: none">-Endpoint data corruption-Limited data breach-Collateral damage	<ul style="list-style-type: none">-Significant revenue loss-Major productivity loss-Extensive system restoration-Large data exfiltration-Increased regulatory scrutiny

**\$5.6M demand
paid in 2019**

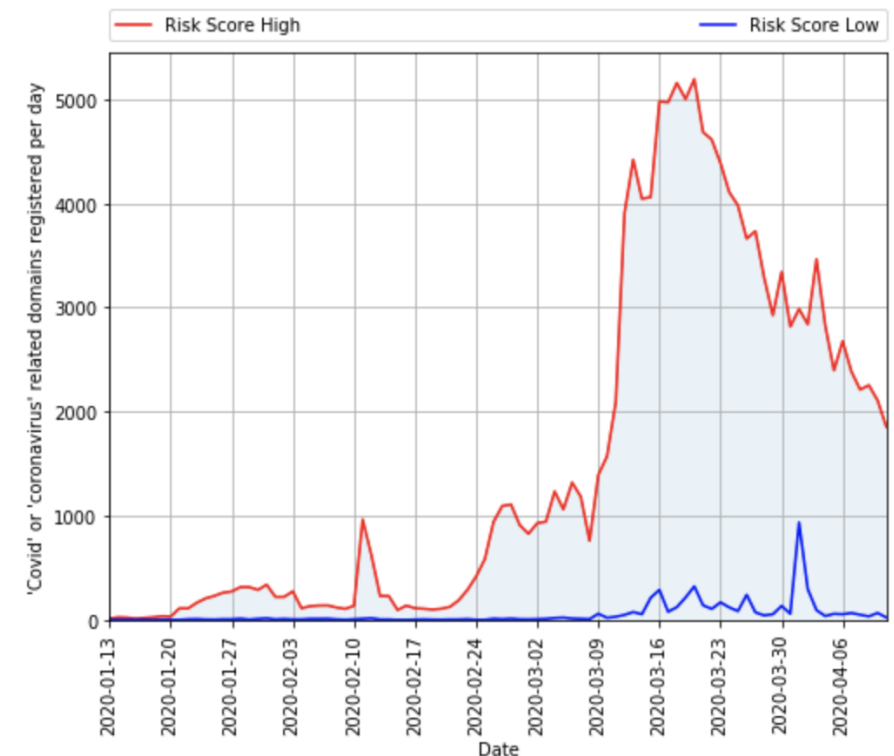
(Source: BakerHostetler 2020 DSIR Report)

Ransomware attack vectors



- Email phishing and misconfigured RDP ports are the most prevalent attack vectors for ransomware
- Researchers have observed a sharp increase in suspicious COVID-themed emails and websites
- Cyber criminals are actively targeting points of aggregation to launch attacks at a much larger scale (e.g., managed IT service providers)

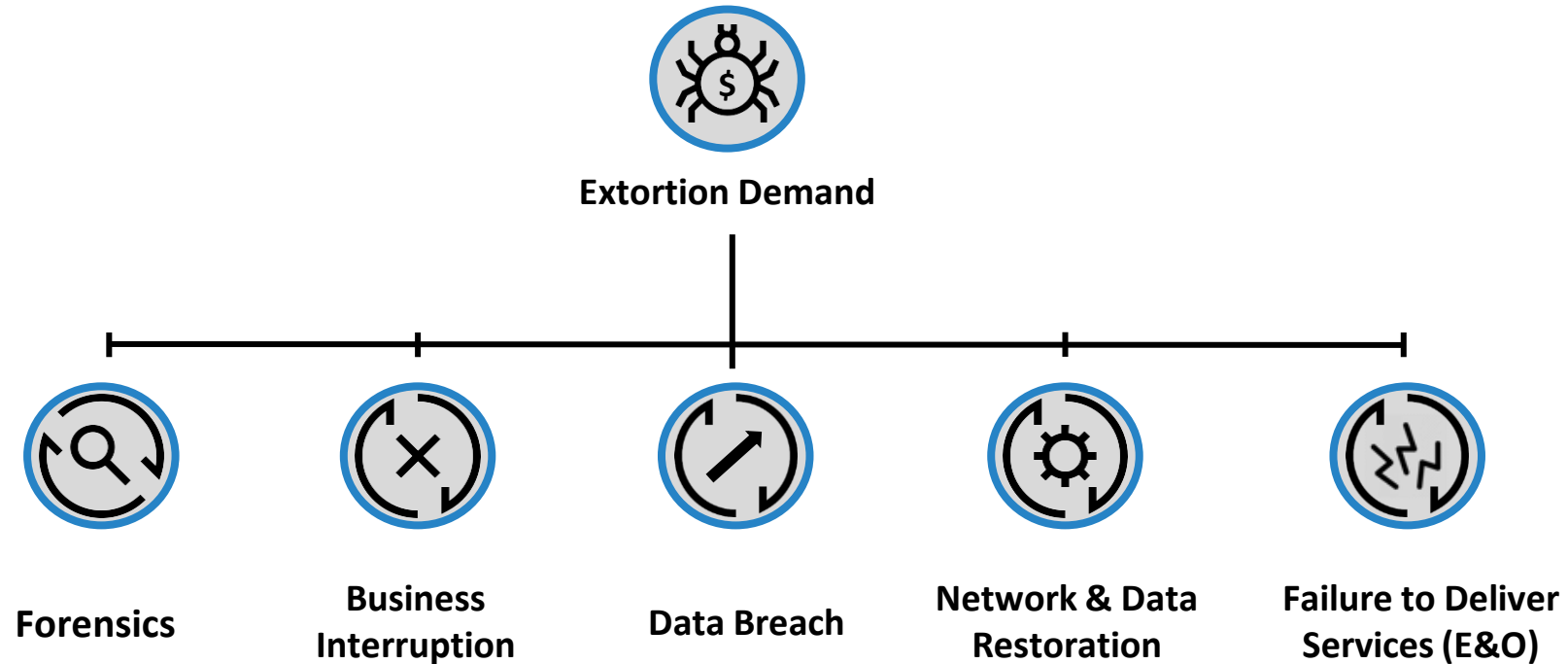
COVID-themed domain trends



(Source: Cyber Threat Coalition / DomainTools)

Ransomware is more than extortion

Ransomware often triggers multiple coverages which increase the severity of loss



Business Interruption



- The severity of BI events has increased due to ransomware & outsourced IT services
 - Data restoration is contributing to productivity loss and extra expense
 - Revenue loss requires forensic accounting
- Industries once viewed as “low risk” due to minimal data privacy concerns have shown high exposure to BI events and the market is reacting
- Business interruption extends beyond network security events
 - Dependent Business Interruption
 - System Failure
 - Dependent System Failure
 - Non-IT Provider Systems
- Understand how BI retentions can vary (waiting periods + dollar (\$) retentions)

Industries hit hardest by ransomware

- Manufacturing
- Prof. Services
- Healthcare
- Public Entities

Financial Fraud

- Email is the predominant attack vector - cyber criminals research victims and execute targeted phishing campaigns
- Companies that transact at high volume are more susceptible to financial fraud - it's easier for suspicious activity to go unnoticed
- Business email compromise (BEC) increases the risk of both first and third party wire fraud loss

Coverage Spotlight



SOCIAL ENGINEERING

Ensure no call-backs, check for coverage of 'other property' and scope of who's funds are covered

CLIENT ACCOUNT / INVOICE MANIPULATION

Third-party social engineering coverage triggered by fraudulent invoices being sent from insured's email

FUNDS HELD IN ESCROW

Some policy forms only cover 'your' funds, not the funds of others in your possession



**\$264,117 avg.
stolen in 2019**

(Source: Crypsis 2020 Incident Response & Data Breach Report)

Common Policy Issues / Exclusions to Avoid

! **Breach Costs – Reimbursement vs Pay on Behalf**

Many policy forms offer to reimburse the insured for these expenses, but still require you to utilize their vendors. Most SME companies don't have the funds to front this cost.

! **Full Prior Acts / Lingering Undetected Malware**

New retro date can exclude previously undiscovered events if wording is not written on a "First Discovered" basis (vs "First Occurred") or with a retroactive date of "Full Prior Acts".

! **Data Restoration Coverage Differences**

Many forms don't cover data recreation, only coping and backup media (very cheap).

! **Inadequate PII Definitions**

Insureds want coverage triggered for any exposure of non-public personal information, not the carrier's opinion as to what defines PII

! **Definition of Network**

Many forms require a contract to be in place with outsourced providers storing your data. Most businesses have 4th and 5th parties that hold their data and don't realize this fact.

! **Breach of Contract Exclusions**

Consider policy wording when signing contracts with indemnification language.

- Non-Disclosure Agreements
- Confidentiality Agreements
- Service Level Agreements
- Business Associate Agreements
- Merchant Services Agreements

Common Policy Issues / Exclusions to Avoid

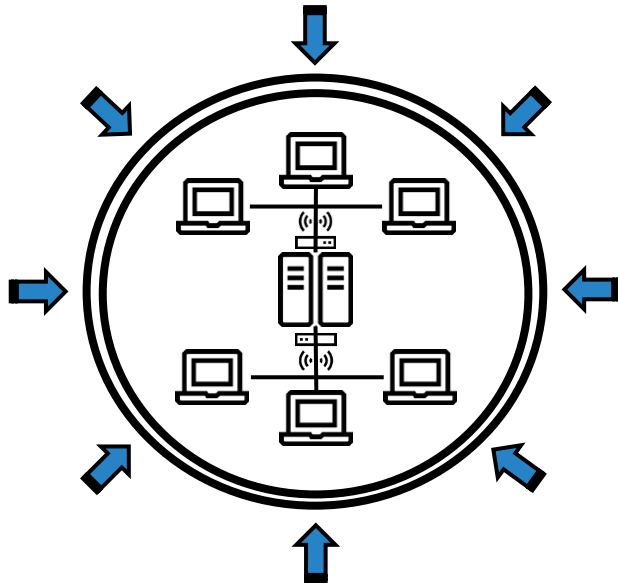
- ! **Laptop Breaches** confined to devices that are in your “Direct and Continuous Physical Control.”
- ! **Coverage Applies to the Insured’s “Network”** specifically carves out coverage for any public infrastructure (cloud, e-mail, databases, outsourced hosted software, etc.). Offline data could be excluded.
- ! **Nonpublic Personal Information** is defined as “two or more elements of information not available to the general public...”
- ! **Privacy Event Expenses** applies to a breach notice law, on a reimbursement basis.
- ! **Privacy Regulatory Coverage** Only newer policy forms will address regulatory violations not triggered by a data breach, rather the misuse of data. New laws and regulations need constant evaluation.
- ! **Intellectual Property** If insured is responsible for securing third-party IP, coverage may not apply.
- ! **Broad Exclusion** for the failure of products/services (doesn’t specifically state the insured’s products/ services). Could exclude coverage for a breach due to a failure in performance of a security product.
- ! **Malfunction or Error** is any mechanical failure, faulty construction, error in design, latent defect, wear or tear, gradual deterioration, electrical disturbance, Storage Media failure or breakdown or any malfunction or error in programming or error or omission in processing.
- ! **Social Engineering** requires a ‘call-back’ out-of-band verification for social engineering coverage to actually be triggered (which removes almost all need for the coverage in the first place).



Cyber Prevention & Recovery

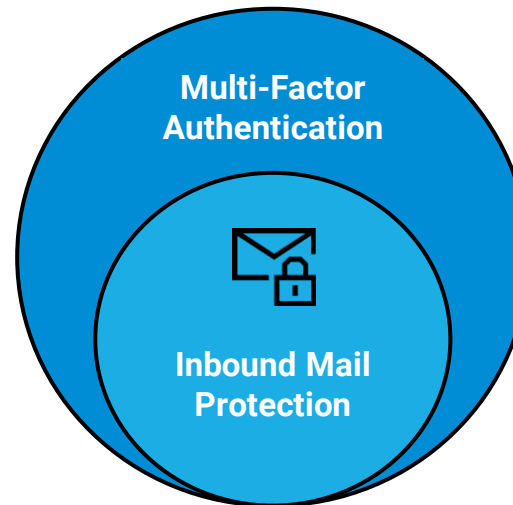
Solid prevention is multi-layered

Keep a clear perimeter



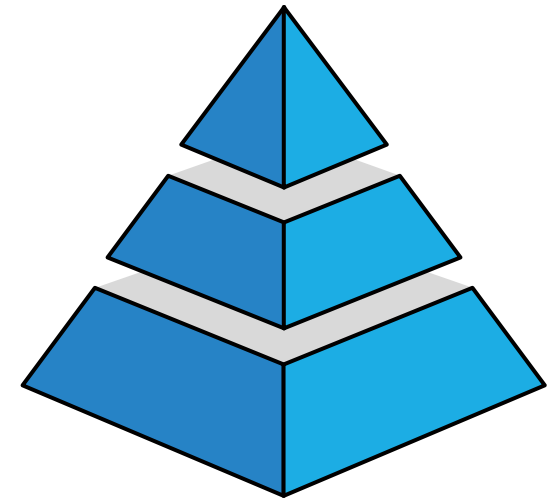
- Avoid end of life systems
- Patch known vulnerabilities
- Keep databases off perimeter
- Close remote desktop access

Stop attackers at the gate



- Enable MFA on email and remote access tools
- Securely configure email and use filtering technology

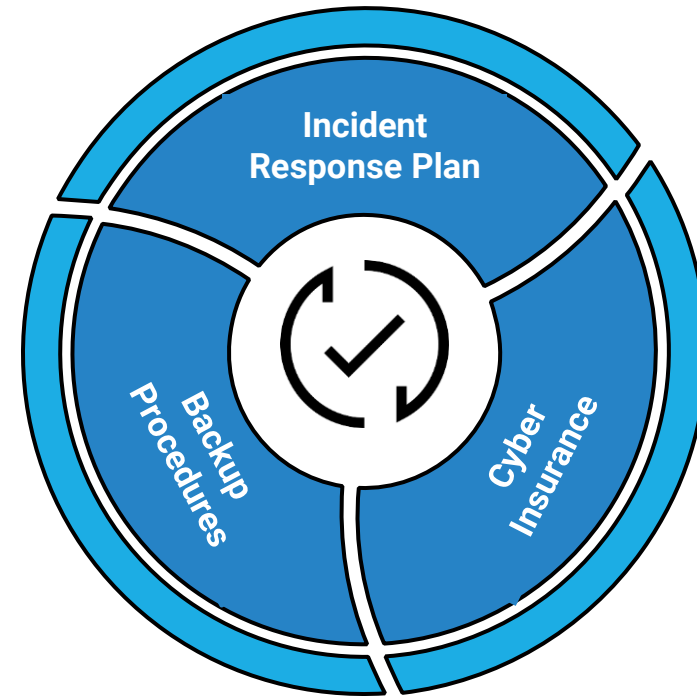
Implement procedures



- Data access controls
- Funds transfer protocols
- The "human firewall"

Preparation is key to recovery

- Have a documented plan and regularly test it
- Segregate and maintain multiple sources of backups
- Cyber insurance can protect your bottom line





Future of Cyber Insurance

Insurers are focusing on technology



Photo by Kevin Ku on Unsplash

Insurers are leveraging technology to...

- Enhance the underwriting process
- Verify security controls
- Identify vulnerabilities
- Collect data for actionable intelligence
- Create better products and services



Worldwide Facilities[®], LLC

Thank you for participating in today's presentation.

*For additional information, reach out to Matt Donovan at (678) 502-1278
or email mdonovan@wwfi.com*