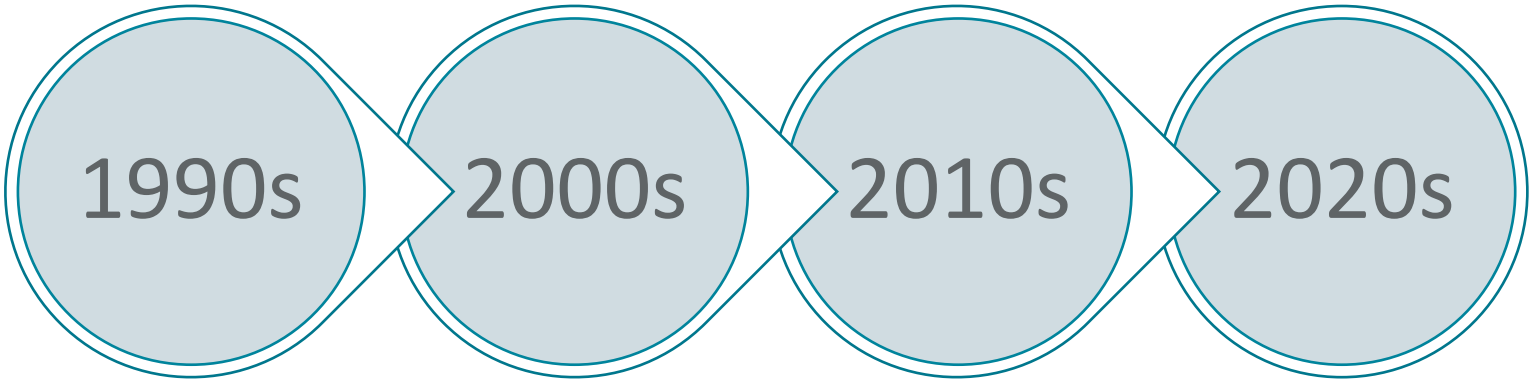
CYBER LIABILITY

WTBA 2022 Annual Convention

THE INTERNET IN 1994

THE EVOLUTION OF CYBER EXPOSURE



- Y2K Concerns
- Increased Reliance on the Internet
- Regulatory Environment Changing
- Business Impact

PROFITABLE BUSINESS

$6 Trillion:
The projected impact of cyber crime in 2021[1]

Every 2 Seconds:
There is a new victim of identity theft in the US[2]

$3.86 Million:
Global average cost of a data breach, increasing to $8.64M in the US[3]

16 Billion:
Estimated records exposed in data breaches since 2019[2]

63%:
Of organizations experience a breach with a loss of 1000+ records[4]

$302,539:
Average ransom payment to cyber criminals[4]

31%:
Percentage of data breach victims who later have their identity stolen[2]

$2 Million:
Average cost savings from having an established incident response team with a tested plan[3]

1. CisionPR Newswire, April 2020
2. Self Key, July 2020
3. Ibm Security, cost of a Data Breach Report, 2020
4. IBM and Ponemon, cost of a Data Breach Report, 2020

M3 INSURANCE

2022

Cyber Risk News

- Accellion May Pay $8M For Data Breach That Spooked BigLaw
  01/13/2022
- Morgan Stanley to settle data breach lawsuit for $60M
  01/03/2022
- Twitter Accounts Of Indian Medical Association, Council Of World Affairs Hacked
  01/03/2022
- Broward Health Network Breached, Hacker Gains Access to Private Patient Information
  01/02/2022
- N Korean hackers stole $1.7 billion from cryptocurrency exchanges
  01/01/2022
- Pulse TV reports about 200,000 credit card credentials hacked
  01/01/2022

INSURANCE

CONSTRUCTION

- Drones/Portable Devices
- Wearable Equipment
- Confidential Project Information
- Trade Secrets/IP
- Miss Bid Day
- Real Estate – smart communication
- Payroll Software
- Cloud Systems/Third Party Storage

M3 INSURANCE

TOP THREE CLAIMS TRIGGERS

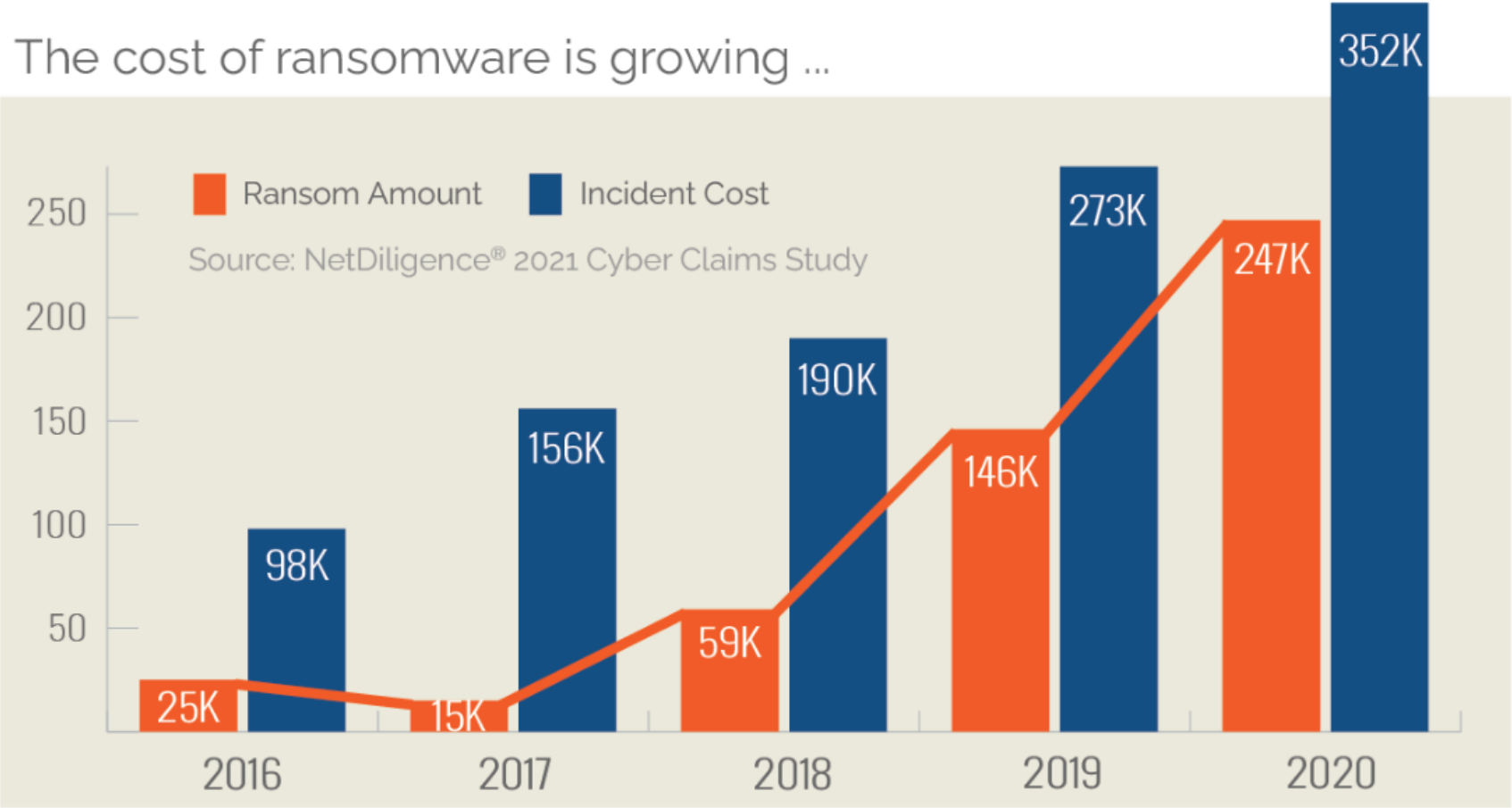
Social Engineering

Business Email Compromise

Ransomware

M3 INSURANCE

The cost of ransomware is growing ...



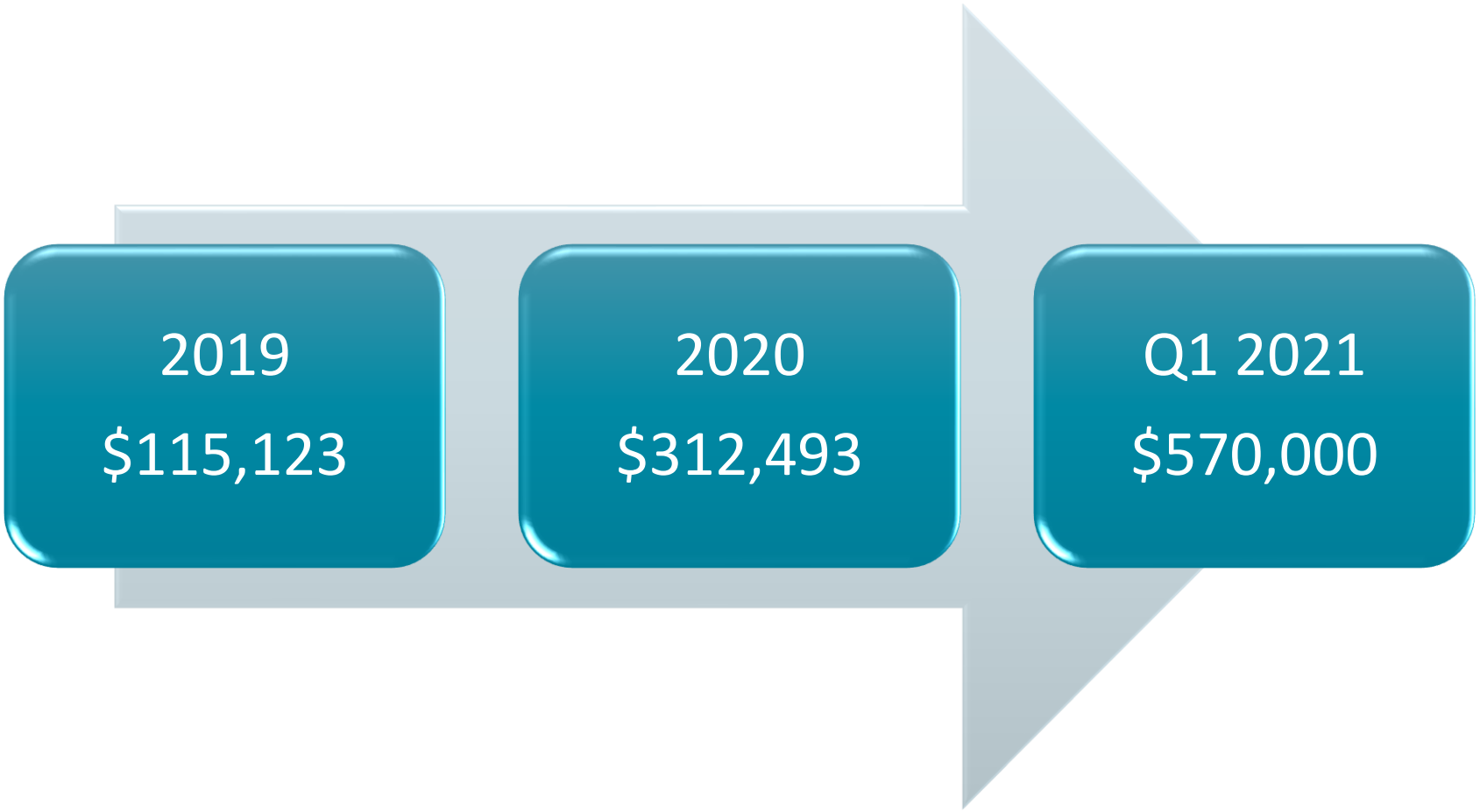
M3 INSURANCE

RANSOMWARE

A type of malicious software designed to block access to a computer system until a sum of money or other consideration is paid.

- Exploit kits – via compromised websites and malvertising
- Malicious email attachments
- Malicious email links
- Social media and SMS
- Ransomware-as-a-Service (RaaS)

AVERAGE RANSOMWARE PAYMENTS



SOCIAL ENGINEERING

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes

- Phishing Emails
- Vishing
- SMShing
- Water Holing
- Tailgating

CREDENTIAL HARVESTING

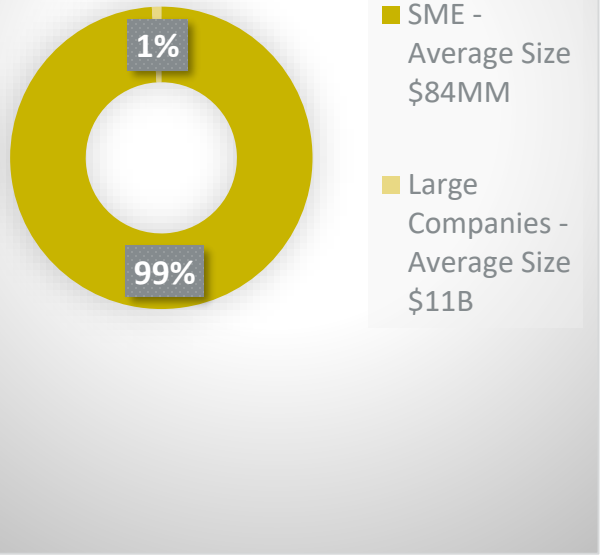
Gathers valid usernames, passwords, private emails, and email addresses through social engineering techniques, digital scamming (including phishing) and malware.

- Fake websites
- Fake SMS messages
- Phishing emails
- Skimming from compromised websites
- Social engineering

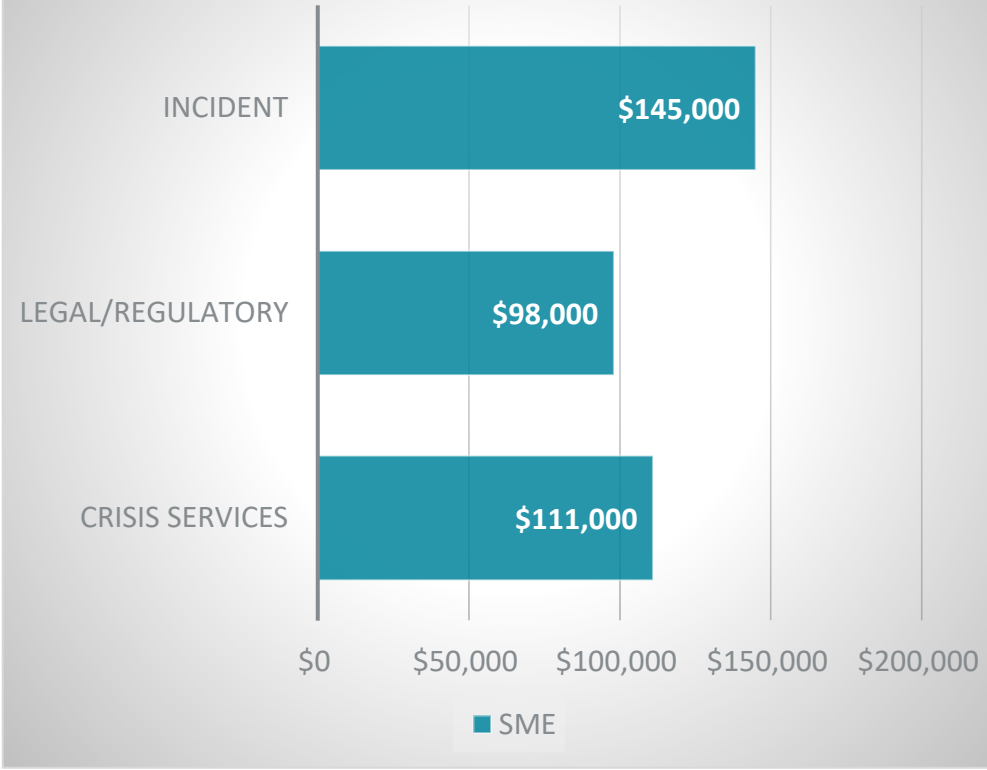
INSURANCE

CLAIMS TRENDS

Company Size

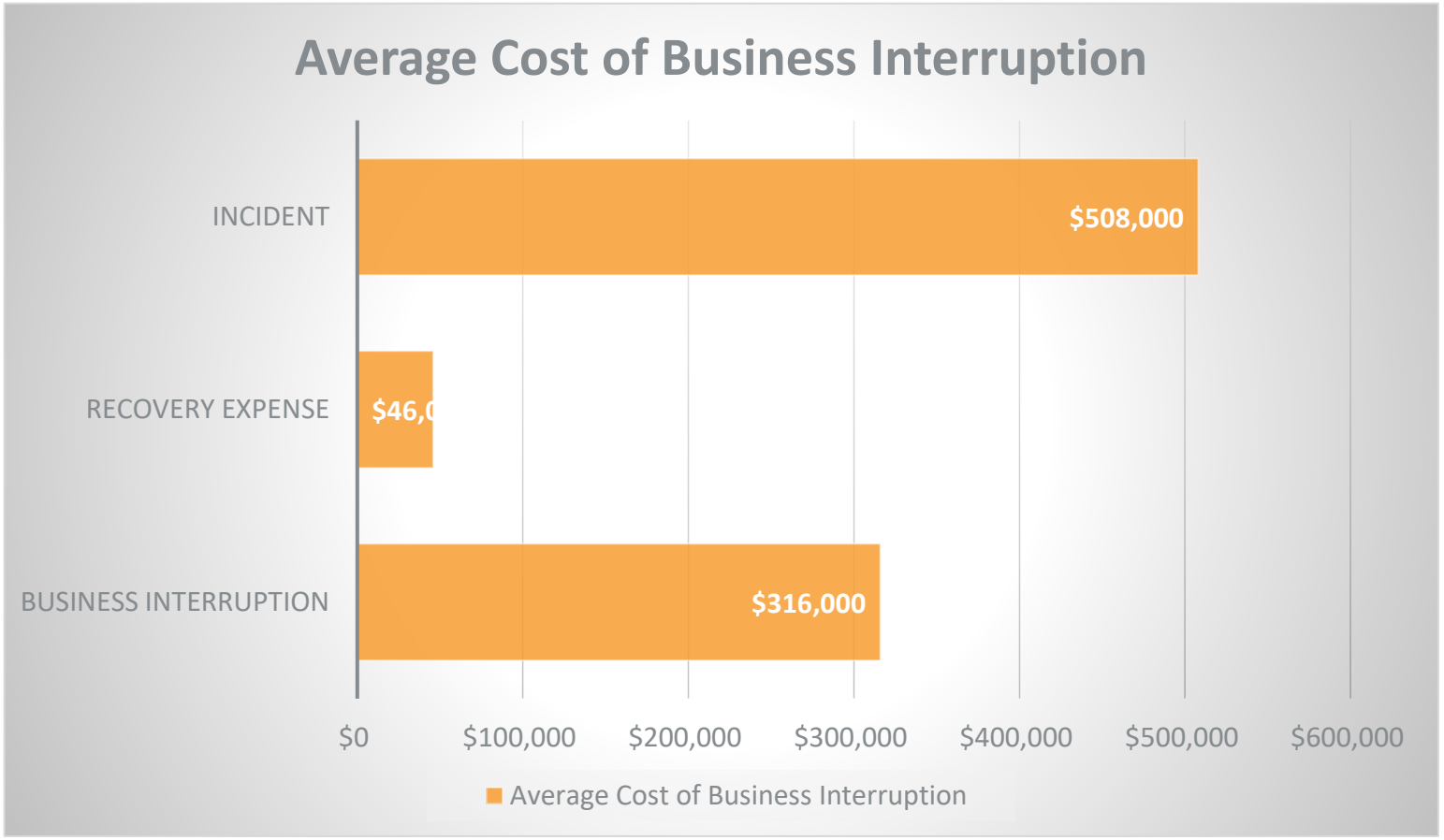


Average Cost of a Claim



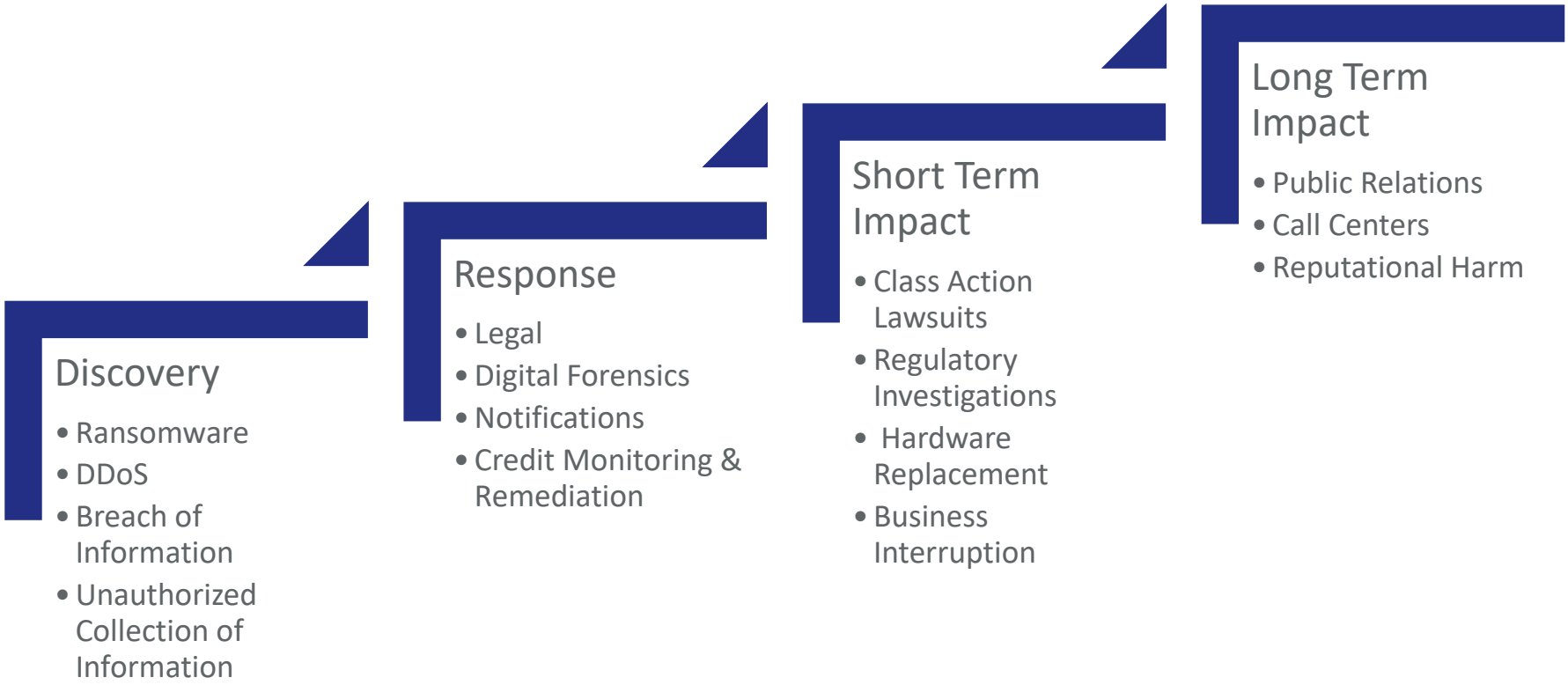
Source: NetDiligence Cost of a Cyber Claim Study 2021

CLAIMS TRENDS



Source: NetDiligence Cost of a Cyber Claim Study 2021

THE ANATOMY OF A BREACH



M3 INSURANCE

BEST PRACTICES AFTER AN INCIDENT

- Refer to incident response plan
- Do not communicate internally or externally (the attorney will advise on communications)
- Utilize personal emails instead of work emails
- Phone calls are best form of communication
- Contact insurance carrier to start claims process

STATE OF THE MARKETPLACE

Pricing & Capacity

- Hard pricing environment – 50%-100% increases
- Prescriptive risk control measures
- More limited capacity
- Third party analytics

Markets

- Reinsurance has become more limited
- Carriers' appetites continue to change and evolve
- InsureTech continues to expand

Coverage

- Some carriers are sublimiting Cyber Extortion (ransomware) coverages
- Many carriers are re-filing their forms

M3 INSURANCE

EVOLVEMENT OF CYBER RENEWAL

SERVICE	DESCRIPTION	INTERNET FACING	MFA REQUIRED	SUGGESTED ACTION
EMAIL	Email SaaS Platform(s) O365/Google	YES	YES	Cloud/Internet facing email services must utilize MFA. (Office 365/Exchange On-Line (EOL), Google Workspace, Yahoo, etc.) Most of the bigger SaaS services/platforms have MFA built into them. It only requires turning the features on and training users.
	Email services Web-hosted/Internet Service Provider (ISP)	YES	YES	Hosted/ISP email services by default are internet-facing and require a second factor beyond username/password. (Rackspace, Comcast, Verizon, etc.) Most have the ability to enable MFA. If not, it might require migrating to a more secure platform.
	Email Servers On-Premises	PARTIAL	YES – WHEN WEB ACCESS IS ALLOWED	On-Premises email servers that are 100% behind your organizations firewall DO NOT require MFA. (Exchange, Lotus Notes, Postfix, Zimbra, etc.) However, if you allow web access such as MS Exchange Outlook Web Access (OWA) or Mobile Devices to access email such as MS ActiveSync then MFA and other Mobile Device Management (MDM) protections should be in place.
REMOTE ACCESS	Virtual Private Network (VPN) Access	YES	YES	To enhance security on VPNs, utilize additional factors beyond username/passwords. VPN is a secure encrypted gateway/pathway directly into your organization's on-premise network from outside.
	Remote Desktop support tools	YES	YES	Remote Desktop tools (LogMeIn, Splashtop, GoToMyPC, Teamviewer, etc.) should all have MFA enabled on their management portals. These tools provide remote access directly into your organization's on-premises network by allowing direct access to Servers/Desktops/Laptops/VMs.
	Managed Service Providers (MSPs) use Remote Management & Monitoring (RMM) tools	YES	YES	MSPs use RMM tools (ConnectWise, NinjaRMM, Kaseya, Atera, MS Intune, etc.) which should have MFA enabled. These tools provide third-party MSPs access directly into your organization's network. Specifically, they can get onto Servers/Desktops/Laptops/Virtual Machines/Network Equipment, etc. These RMM tools are secure and encrypted but should require MFA to gain access.
	Virtual and Application Gateways	YES	YES	Virtual gateways like VMWare's Horizon, Citrix Virtual gateways or other MFA/IdP (Identity Provider) application gateways that allow direct access from the internet to virtual machines or applications inside your network should all require MFA. These solutions are internet facing and therefore require MFA.
DIRECTORY SERVICES	Microsoft Active Directory, LDAP	NO	YES	Requiring that Domain Admin level credentials are challenged with MFA makes it much harder for nefarious actors to easily gain privileged access on your systems and network. Additionally, challenging Identity internally helps restrict bad actors from stealing elevated credentials, executing ransomware payloads and makes lateral movement much more difficult.
BACKUPS	Backup software management	NO	YES	The management console of your backups should be protected with MFA. (Veeam, Datto, Veritas, Barracuda Backup, etc.) Your backups should be protected in transport using encrypted transport protocols; you also need to ensure that your backups are stored securely using either encryption, strict Role-Based Access Controls (RBAC) or airgap measures. The final step is using MFA to protect the management console.

SERVICE	DESCRIPTION	INTERNET FACING	MFA REQUIRED	SUGGESTED ACTION
NETWORK INFRASTRUCTURE	Firewall, Router, Switch, Hub and Wireless Access Point Management	NO	YES	The management console of network equipment should be protected with MFA. There are several ways to protect access. First, all the MFA/IdP providers use an Authentication RADIUS Proxy. Any system that is RADIUS Authentication capable can be paired up with an Auth Proxy. Many Firewall/Router/Switch brands have the built-in ability to turn on a second factor as well. Lastly, using/creating a management network by segmentation/IP restrictions and using an access gateway protected with MFA is acceptable architecture, too.
ENPOINTS	Servers, Desktops, Laptops, Virtual Machines	NO	YES	All local and domain level administrator access to endpoints should be protected with MFA. (Cisco Duo, OKTA, OneLogin, Ping, WatchGuard, AuthLite, UserLock, etc.) Most MFA/IdP providers have operating system clients that when coupled with LDAP synchronization and an Identity Portal allow for MFA challenges when logging into endpoints with elevated accounts.

M3 INSURANCE

PREVENTATIVE CONTROLS TO CONSIDER

Multi-Factor Authentication	Endpoint Detection Software	Incident Response Planning
Closing/Securing Open Ports	Encryption	Redundancies and Back-Ups
Oversight of Payment Controls	Complex Password Requirements	Employee Training

M3 INSURANCE

QUESTIONS?

Director of Construction & Real Estate
Brad Winchester
brad.winchester@m3ins.com

M3 INSURANCE