Memorandum

MONTANA
DEPARTMENT OF COMMERCE

TO: EWAC Working Group
Scott Osterman, DOC Director
FROM: Liane Taylor, Business MT DA
DATE: September 13, 2022
SUBJECT: Cybersecurity Monitoring, Security and Training

Overview: The appropriation in this section may be used for eligible business transformation and stabilization and workforce development programs, including but not limited to workforce training including rapid retraining, return-to-work bonuses, or short-term wage subsidies, business assistance for hiring or rehiring employees, business assistance for training or retraining employees, business technology grants, agricultural resiliency, and business transformation or stabilization grants.

The goal of this program is to provide much needed awareness regarding the threat of cybersecurity as well as monitoring, security and training to protect Montana's small and medium sized businesses from cybersecurity attacks.

According to 2022 Must-Know Cyber Attack Statistics and Trends
https://www.embroker.com/blog/cyber-attack-statistics

Cyber-attacks on all businesses, but particularly small to medium sized businesses, are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyber-attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

Not only does a cyber-attack disrupt normal operations, but it may cause damage to important IT assets and infrastructure that can be impossible to recover from without the budget or resources to do so.

Small businesses are struggling to defend themselves because of this. According to Ponemon Institute's State of Cybersecurity Report, small to medium sized business around the globe report recent experiences with cyber-attacks:

Insufficient security measures: 45% say that their processes are ineffective at mitigating attacks.
Frequency of attacks: 66% have experienced a cyber-attack in the past 12 months.
Background of attacks: 69% say that cyber-attacks are becoming more targeted.

The most common types of attacks on small businesses include:

Phishing/Social Engineering: 57%
Compromised/Stolen Devices: 33%
Credential Theft: 30%

Allocation Request: $2.2M

Structure: $2 million would be provided in cybersecurity monitoring and security. Businesses would receive up to $2,500 in grant funds to be paid to an accredited Montana cybersecurity company for monitoring and security equipment/programs.

$250,000 for reimbursement to businesses. Missoula College has a new program specifically for businesses for yearlong monthly cybertraining with certification badge upon completion. This would help businesses get insurance certification. Annual cost is $20/pp. Businesses would then attach certifications for reimbursement. See attached program flyer.

Eligibility: See attached guidelines

Performance Metrics*: 10,000 employees badged.*

Recommendation:
Allocate $2.2 M in reallocated workforce training funds to provide cybersecurity monitoring and security to businesses. Provide training to business employees.

CYBER MONTANA

UNIVERSITY OF MONTANA
MISSOULA COLLEGE

Customized Cyber Awareness Training for Small and Midsize Montana Business

The greatest vulnerability to cyber-attacks is the human factor. **Nearly 90% of cybersecurity issues are caused by human error.** Preventing cyber-attacks begins with employee education, which is essential in constructing a defensive cyber posture for reducing cyber risk. Educating users can drive behavior change and ensure that employees have the right response to security or privacy threats.

Small and midsize businesses (SMB) are the backbone of the Montana economy. While education programs have been deployed for larger institutions, training resources for SMBs are limited. **CyberMontana recognizes Montana's greatest cyber vulnerability and has developed customized cyber awareness training with the specific focus of addressing Montana's SMBs.**

The **CyberMontana Security Awareness training program** uses a research-based methodology to educate the SMB workforce through **20-30 minute monthly lessons** on relevant topics such as phishing, password management, safely using public wireless networks, and best practices for remote workers. By completing a 12-month training program, **employees earn a digital badge in cyber readiness**. At the same time, **businesses can be validated as being cyber-ready** having reduced their cyber vulnerability through employee education.

The CyberMontana employee end-user training program is **modestly priced with an annual cost of $20/user**.

The request for the Montana Department of Commerce is to enhance cybersecurity for Montana SMBs by promoting business validation through the CyberMontana Security Awareness training program. Funding is needed to reimburse participating businesses for training expenses. Our goal would be to provide the opportunity to **badge 10,000 or more SMB employees for completing end-user cyber training**. It will require funding to create a SMB cyber readiness validation program through employee training. **We request employer reimbursement funding of $250,000. All monies would be managed by the Montana Department of Commerce** and go directly to businesses choosing to enhance their cybersecurity defensive posture through the CyberMontana employee education program.

SNAP DEFENSE

ANDERSON ZURMUEHLEN

PRICING Charged per managed endpoint

INCLUDED FEATURES
- Live Asset Visibility
- Multi-Point Threat Detection
- Realtime Threat Response
- Privileged User Visibility
- Multi-Tenant for MSSPs
- Risk and Compliance Reporting
- Simplified Deployment and Management

OPTIONAL ADD-ON OT/BAS/ICS Asset Visibility, Monitoring, and Protection with NICOS Module

LIVE ASSET VISIBILITY

Visualize Alerts and Hunt Threats in Realtime Within the Context of your OT/IT Infrastructure

- Live network map of Cisco, Juniper, endhost, server, mobile, and IoT devices
- Live alert visualization with network context
- Operational Technology (OT), Building Automation Systems (BAS), and Industrial Control Systems (ICS) asset discovery and mapping (with NICOS)
- Automatically generates Layer-2 and Layer-3 links using ARP, MAC tables, CDP, IP/Subnets, and DHCP (with NICOS)
- View integrated map of IT and OT assets
- Displays managed and unmanaged devices
- Displays Wi-Fi connected devices, including support for Meraki API
- Collects endpoint and router metadata, including running services and processes, netstats, users, configuration files, and more
- Provides on-demand device metadata collection
- Point-and-click down selection and filtering
- Quickly search device metadata, including services, processes, users, OS versions, etc.
- View up/down status for managed devices
- Detailed VLAN and subnet visibility, including endhost to VLAN mapping
- 3rd party product integration, including SIEM, anti-malware, and traffic analysis

MULTI-POINT THREAT DETECTION

Identify Threats in Realtime Using SNAP Patented Detection Technology

- Immediate lateral spread detection
- Immediate remote privileged activity detection
- Immediate network enumeration detection
- Immediate malware event detection (with anti-malware integration)
- Immediate process hash and process tree visibility during an alert
- Immediate removable storage detection
- Immediate syslog-based threat alerting with automated context enrichment
- Continuous and custom monitoring of Windows process and service threat indicators
- Automated alert correlation and enrichment, including affected devices' users, VLANs, hostnames, OS versions, and more
- Customizable suppression rules reduce threat event operator/analyst overload
- Realtime SMS and email threat notifications
- Integrates, consolidates, and enriches alerts from numerous 3rd party security applications, including Sophos, Cisco AMP, Meraki, and more

SNAP DEFENSE

ANDERSON ZURMUEHLEN

REALTIME THREAT RESPONSE

Stop Threats in Realtime with Built-in, Immediate, and Effective Response

- Point-and-click response to detain compromised devices
- Easily understandable alerts enable rapid triage by Tier 1 analysts with detailed data for Tier 3 analysts
- Custom detainment notification message to device users
- Immediate notifications of un-detained devices
- Preserves compromised device state for follow-up forensics and threat analysis
- 3rd party response orchestration

PRIVILEGED USER VISIBILITY

Gain Unparalleled Live Insight into Privileged User Activity and Behavior

- Identify privileged user accounts
- View privileged user activity, including network shares, remote desktop, remote execution, and more
- Detect low-frequency privileged activity
- Automatically reports new, previously unseen privileged users and activity
- Immediately identify privileged insider threat

MULTI-TENANT FOR MSSPS

Manage Multiple Client Networks with a Single Installation and User Interface

- Consolidated alert and system status dashboard
- On-Prem, hybrid on-prem, or Blackpoint cloud provided hosting
- Monthly billing
- Rapid deployment to quickly add new clients
- Sales and marketing support
- Ideal for Hunt as a Service, Compliance as a Service, Incident Response, Continuous Monitoring, Network Security Assessments, and more

RISK AND COMPLIANCE REPORTING

Identify Security Risks and Ensure Continuous Compliance

- Quickly generate real-time and historical reports

SUMMARY REPORT:

- Outstanding alerts by criticality, type, and time
- Overall system health and status
- Suppressed events by type and time

COMPLIANCE REPORT:

- PCI-DSS
- HIPAA
- NIST 800-171
- NYCRR-500
- Sarbanes-Oxley (FY19)
- CJIS (FY19)
- CIP-NERC (FY19)

PRIVILEGED ACTIVITY REPORT:

- New/most/least active privileged users
- New/all remote executions
- Remote executions by user and application
- New/all RDP activity
- RDP activity by user, source, and destination
- New/all privileged share activity

SECURITY EVENTS REPORT:

- Anti-malware events by severity, type, and time
- Process and service threats by severity, type, and device
- New attack sources and targeted devices
- New point-to-point connections
- New/all USB activity
- USB activity by device
- New/all malware persistence techniques

NETWORK REPORT:

- Detected enumeration activity
- Enumeration activity by source, destination, and time
- Core network change detection
- SNMP community strings
- Insecure core network passwords
- Network Management devices, including TACACS, SNMP, NETFLOW, SYSLOG, NTP, and RADIUS

SNAP DEFENSE

ANDERSON
ZURMUEHLEN

REALTIME THREAT RESPONSE

Stop Threats in Realtime with Built-in, Immediate, and Effective Response

- Point-and-click response to detain compromised devices
- Easily understandable alerts enable rapid triage by Tier 1 analysts with detailed data for Tier 3 analysts
- Custom detainment notification message to device users
- Immediate notifications of un-detained devices
- Preserves compromised device state for follow-up forensics and threat analysis
- 3rd party response orchestration

PRIVILEGED USER VISIBILITY

Gain Unparalleled Live Insight into Privileged User Activity and Behavior

- Identify privileged user accounts
- View privileged user activity, including network shares, remote desktop, remote execution, and more
- Detect low-frequency privileged activity
- Automatically reports new, previously unseen privileged users and activity
- Immediately identify privileged insider threat

MULTI-TENANT FOR MSSPS

Manage Multiple Client Networks with a Single Installation and User Interface

- Consolidated alert and system status dashboard
- On-Prem, hybrid on-prem, or Blackpoint cloud provided hosting
- Monthly billing
- Rapid deployment to quickly add new clients
- Sales and marketing support
- Ideal for Hunt as a Service, Compliance as a Service, Incident Response, Continuous Monitoring, Network Security Assessments, and more

RISK AND COMPLIANCE REPORTING

Identify Security Risks and Ensure Continuous Compliance

- Quickly generate real-time and historical reports

SUMMARY REPORT:

- Outstanding alerts by criticality, type, and time
- Overall system health and status
- Suppressed events by type and time

COMPLIANCE REPORT:

- PCI-DSS
- HIPAA
- NIST 800-171
- NYCRR-500
- Sarbanes-Oxley (FY19)
- CJIS (FY19)
- CIP-NERC (FY19)

PRIVILEGED ACTIVITY REPORT:

- New/most/least active privileged users
- New/all remote executions
- Remote executions by user and application
- New/all RDP activity
- RDP activity by user, source, and destination
- New/all privileged share activity

SECURITY EVENTS REPORT:

- Anti-malware events by severity, type, and time
- Process and service threats by severity, type, and device
- New attack sources and targeted devices
- New point-to-point connections
- New/all USB activity
- USB activity by device
- New/all malware persistence techniques

NETWORK REPORT:

- Detected enumeration activity
- Enumeration activity by source, destination, and time
- Core network change detection
- SNMP community strings
- Insecure core network passwords
- Network Management devices, including TACACS, SNMP, NETFLOW, SYSLOG, NTP, and RADIUS

SNAP DEFENSE

ANDERSON ZURMUEHLEN

SIMPLIFIED DEPLOYMENT AND MANAGEMENT

Easily Setup, Run, and Manage SNAP

- On-prem, hybrid on-prem, or Blackpoint cloud hosted installations
- Point-and-click automated endpoint deployment
- Real-time system status, including SMS and email notifications
- Robust role-based permission and user management
- Two-factor login authentication
- Point-and-click upgrades

OPTIONAL ADD-ON

NETWORKED INDUSTRIAL CONTROL OPERATIONS SECURITY (NICOS) MODULE

Secure OT/BAS/ICS networks with live-monitoring, visualization, and actionable alerts

- Live OT/ICS/BAS asset mapping and visualization
- Live and customizable auditing and visibility of remote privileged OT/ICS/BAS asset access, including SSH, RDP, VNC, TeamViewer, and more
- Detect known bad traffic and unusual domains
- Detect obfuscated/anonymous traffic (TOR) and port scans
- Protect bi-directional lateral spread between OT and IT networks

	INCLUDED IN PRICE	EXTRA COST
LIVE ASSET VISIBILITY	◉	
MULTI-POINT REALTIME THREAT DETECTION	◉	
REALTIME THREAT RESPONSE	◉	
RISK AND COMPLIANCE REPORTING	◉	
PRIVILEGED USER VISIBILITY	◉	
MULTI-TENANT FOR MSSPs	◉	
SIMPLIFIED DEPLOYMENT AND MANAGEMENT	◉	
OT/BAS/ICS ASSET VISIBILITY, MONITORING AND PROTECTION WITH NICOS MODULE		◉

SNAP DEFENSE

SECURITY OPERATIONS & INCIDENT RESPONSE PLATFORM

ANDERSON ZURMUEHLEN

Today, organizations utilize numerous security products; most are **standalone, complex, and too slow to catch modern day attacks.** Hackers are also relying more on "living-off-the-land" strategies: leveraging existing IT technologies and user accounts for malicious purposes. As a result, detecting and analyzing hacker tradecraft often takes significant time, technical expertise, and resources.

Blackpoint's patented SNAP-Defense security operations and incident response platform is a gamechanger; it excels at monitoring and catching modern hacking tradecraft, delivering real-time alerts, and allowing for immediate threat response.

CAPABILITIES

- LIVE ASSET VISIBILITY
- MULTI-POINT THREAT DETECTION
- LATERAL SPREAD DETECTION
- PRIVILEGED ACCOUNT MONITORING
- IMMEDIATE THREAT RESPONSE
- REMOTE ACCESS MONITORING
- INSIDER THREAT VISIBILITY
- 3RD PARTY INTEGRATIONS
- RISK AND COMPLIANCE REPORTING

AVAILABLE AS:

MANAGED DETECTION + RESPONSE (MDR)

Blackpoint team monitors SNAP-Defense for you

KEY BENEFITS:

- PATENTED LATERAL MOVEMENT DETECTION
- THREAT HUNTING CAPABILITIES
- REAL-TIME THREAT DETECTION AND RESPONSE
- REPORTING AND COMPLIANCE MODULE
- INTEGRATED NON-TRADITIONAL IT ASSET VISIBILITY AND THREAT DETECTION
  - Internet of Things (IoT)
  - Operational Technology (OT)
  - Building Automation Systems (BAS)
  - Industrial Control Systems (ICS)

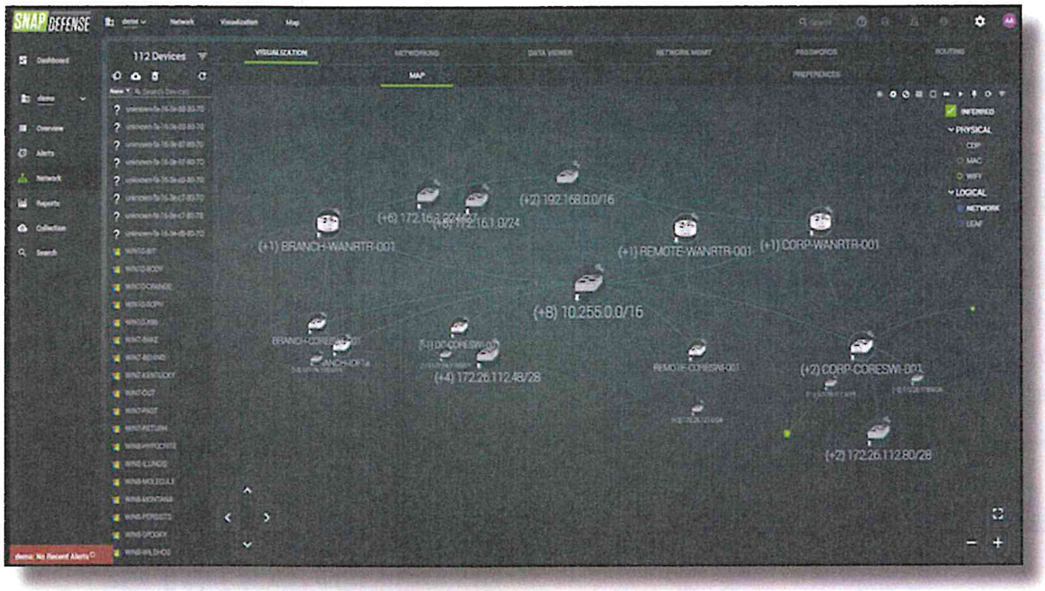
> "SNAP-Defense enables security teams to quickly identify modern hacking tradecraft and take immediate response."
>
> - **JON MURCHISON**, Founder & CEO

866-246-6657 | security@azworld.com | https://azworld.com/services/technology

SNAP DEFENSE

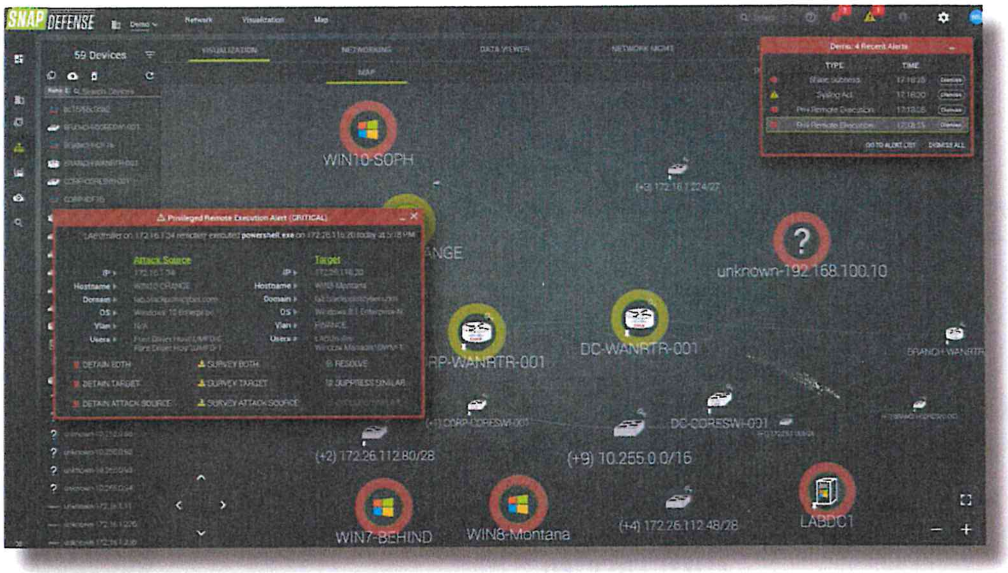
SECURITY OPERATIONS & INCIDENT RESPONSE PLATFORM

ANDERSON ZURMUEHLEN



LIVE ASSET VISIBILITY

IMMEDIATE THREAT RESPONSE



See it in action!

Learn more or schedule a demo by contacting us at the phone or email listed below!

866-246-6657 | security@azworld.com | https://azworld.com/services/technology

Embroker Team August 16, 2022 7 min read

2022 Must-Know Cyber Attack Statistics and Trends

Blog Business Advice & Research

Cyber attacks have been rated the fifth top rated risk in 2020 and become the new norm across public and private sectors. This risky industry continues to grow in 2022 as IoT cyber attacks alone are expected to double by 2025. Plus, the World Economic Forum's 2020 Global Risk Report states that the rate of detection (or prosecution) is as low as 0.05 percent in the U.S.

If you are one of the many that run a growing startup, you know the landscape is ever changing and 2020 brought on several changes, to say the least. The pandemic affected all types of businesses — big and small. If anything, the pandemic amplified cybercrime due to the uncertainty around remote working and how to protect your business.

Cybercrime, which includes everything from theft or embezzlement to data hacking and destruction, is up 600% as a result of the COVID-19 pandemic. Nearly every industry has had to embrace new solutions and it forced companies to adapt, quickly.

How can you prepare your startup for data security in 2022 and beyond? In this guide, we dissect the most important cybersecurity statistics, facts, figures, and trends as they relate to your startup.

The average cost of a si ransomware attack is $1.

million.

Get a free quote to learn how much a cyber insurance policy could save you.

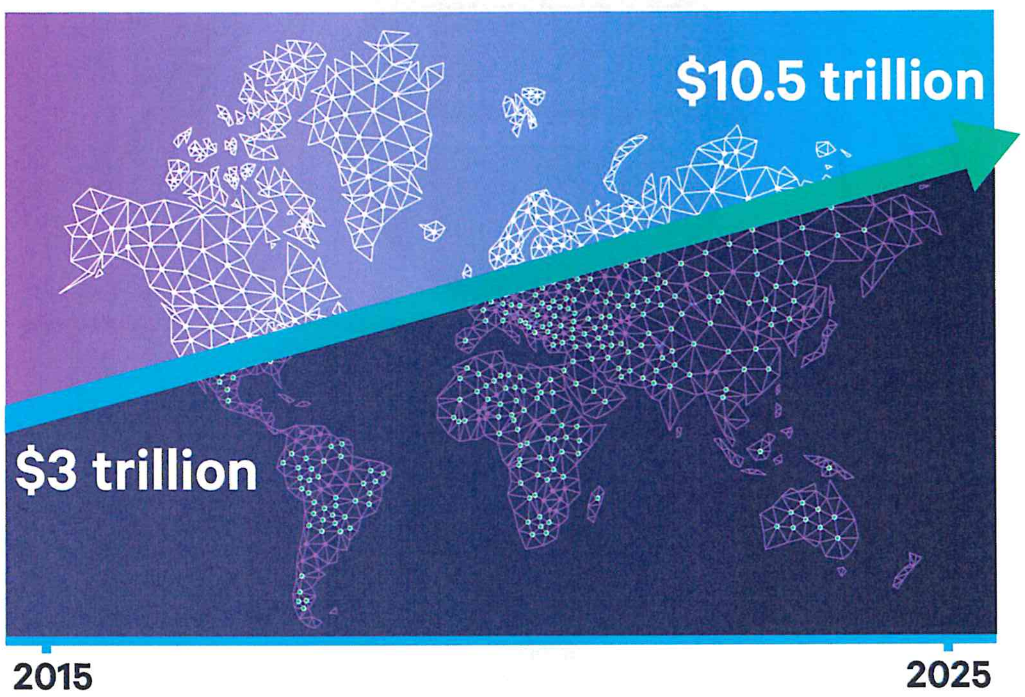
TALK TO A BROKER ☎

Table of Contents

Costs of Cybercrime

Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. At a growth rate of 15 percent year over year — Cybersecurity Ventures also reports that cybercrime represents the greatest transfer of economic wealth in history.

Growth of Cybercrime Costs



Cybercrime for Small and Medium Businesses

Cyber attacks on all businesses, but particularly small to medium sized businesses, are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

Not only does a cyber attack disrupt normal operations, but it may cause damage to important IT assets and infrastructure that can be impossible to recover from without the budget or resources to do so.

Small businesses struggling to defend themselves because of this. According to Ponemon Institute's State of Cybersecurity Report, small to medium sized business around the globe report recent experiences with cyber attacks:

- **Insufficient security measures:** 45% say that their processes are ineffective at mitigating attacks.
- **Frequency of attacks**: 66% have experienced a cyber attack in the past 12 months.
- **Background of attacks**: 69% say that cyber attacks are becoming more targeted.

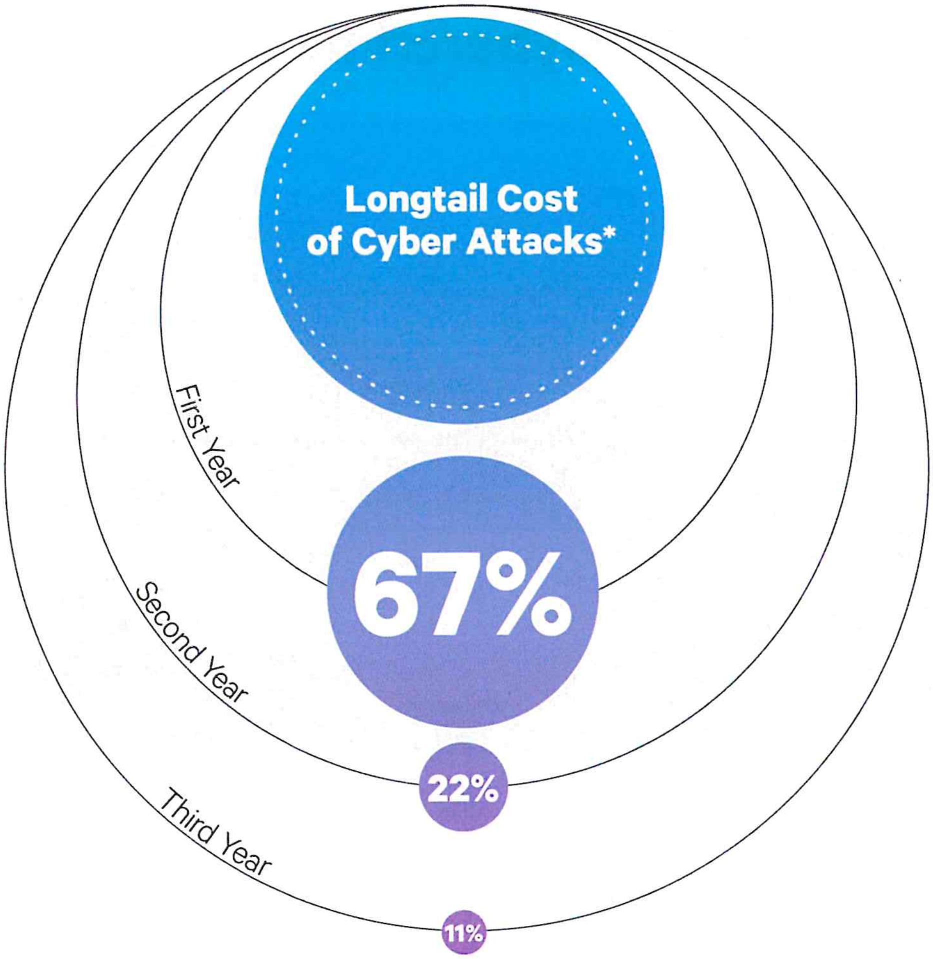
- **Phishing/Social Engineering**: 57%
- **Compromised/Stolen Devices**: 33%
- **Credential Theft**: 30%

By understanding the targets of attacks and consequences, as a business leader you can minimize the potential, gain value in your cybersecurity efforts, and even prevent future attacks.

Longtail Cost of Cyber Attacks

The long tail costs of a data breach can extend for months to years and include significant expenses that companies are not aware of or do not anticipate in their planning.

These costs include lost data, business disruption, revenue losses from system dow costs, or even damage to a brand's reputation. In the visual below, we outline the imp face from the first year up to the third year.



*This includes the costs of lost data, business disruption, revenue losses from system downtime, notification costs and damage to a company's reputation, and the cost of lost customers.

Impact and Severity of Cyber Attacks

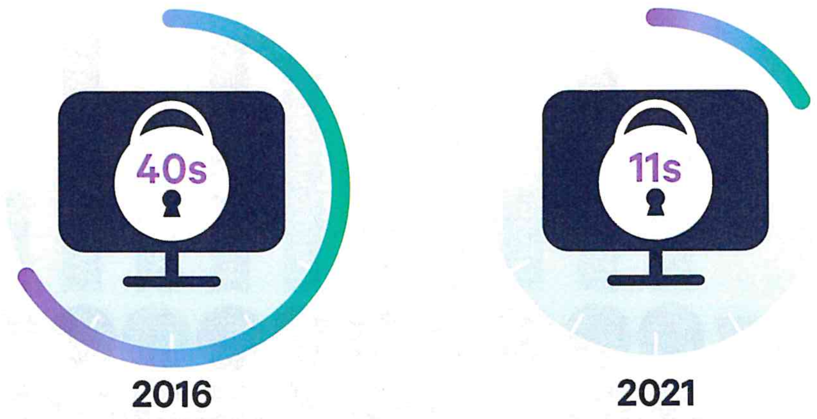
Cyber attacks can impact an organization in many ways — from minor disruptions in operations to major financial losses. Regardless of the type of cyber attack, every consequence has some form of cost, whether monetary or otherwise.

Consequences of the cybersecurity incident may still impact your business weeks, if not months, later. Below are five areas where your business may suffer:

- Financial losses
- Loss of productivity
- Reputation damage
- Legal liability
- Business continuity problems

Ransomware attacks are becoming more prevalent as a concern. At the end of 2016, a business fell victim to a ransomware attack every 40 seconds. This is expected to rise to every 11 seconds by 2021, according to a report by Cybersecurity Ventures. This cyber attack occurs when malicious software is used to restrict access to a computer system or data, until the victim pays ransom requested by the criminal.

Frequency of Ransomware Attacks



Cyber Attacks by Industry

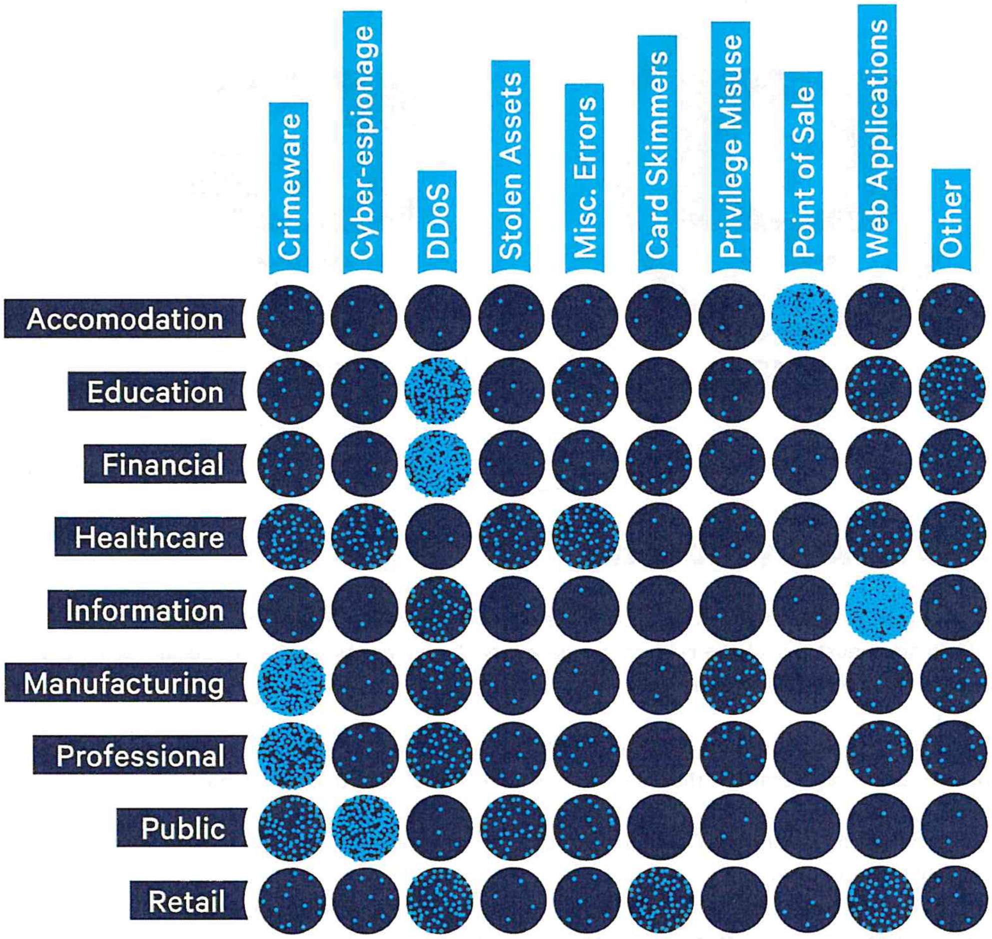
Some industries are more vulnerable to cyber attacks than others, simply due to the nature of their business. While any industry could be subject to a data breach, those most at risk are businesses that are closely involved with people's daily lives.

Companies that hold sensitive data or personally identifiable information are common targets for hackers. Types of businesses or organizations that are most vulnerable to cyber attacks include:

- **Banks and financial institutions:** Contain credit card information, bank account information, and personal customer or client data.
- **Healthcare institutions:** Repositories for health records, clinical research data, and patient records such as social security numbers, billing information, and insurance claims.
- **Corporations**: Has inclusive data such as product concepts, intellectual property, marketing strategies, client and employee databases, contract deals, client pitches, and more.
- **Higher education:** Hold information on enrollment data, academic research, financial records, and personally identifiable information like names, addresses, and billing info.

In the visual below, we break down common types of cyber incidents and the varying impacts on industries.

Cyber Incidents By Industry



(Data covering 2017)

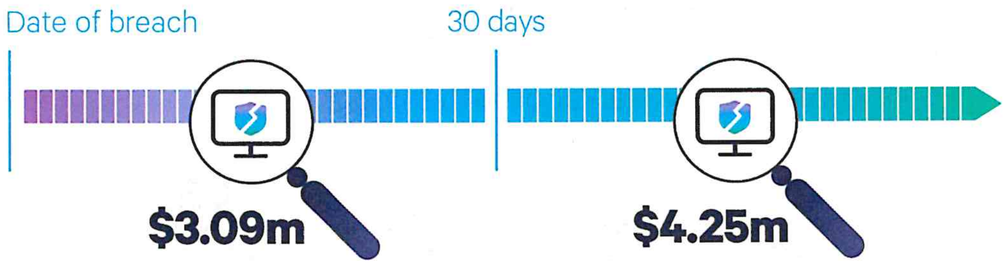
Breach Discovery

Breach discovery is when the company or business becomes aware that the incident occurred. According to IBM, it takes a company 197 days to discover the breach and up to 69 days to contain it.

Companies that contained a breach in less than 30 days saved more than $1 million

compared to those that took more than 30 days. A slow response to a data breach can cause even more trouble for your company. It can result in a loss of customer trust, productivity, or major fines.

Breach Discovery Takes an Average 197 Days



A data breach response plan is a proactive way to be prepared in the event that a breach does occur. Having a risk management strategy in place to combat incidents such as breaches can minimize the impact on your company and bottom line. An incident response plan, for example, provides guidance for your team during the phases of detection, containment, investigation, remediation, and recovery.

Information Security Spending

Global spending on cybersecurity products and services is predicted to exceed $1 trillion cumulatively over the five-year period from 2017 to 2021. This is a 12-15% year-over-year cybersecurity market growth from 2021.

Information Security Spending

Global spending on cybersecurity products and services is predicted to exceed **$1 trillion cumulatively** over the five-year period from 2017 to 2021. This is a 12-15% year-over-year cybersecurity market growth through 2021.

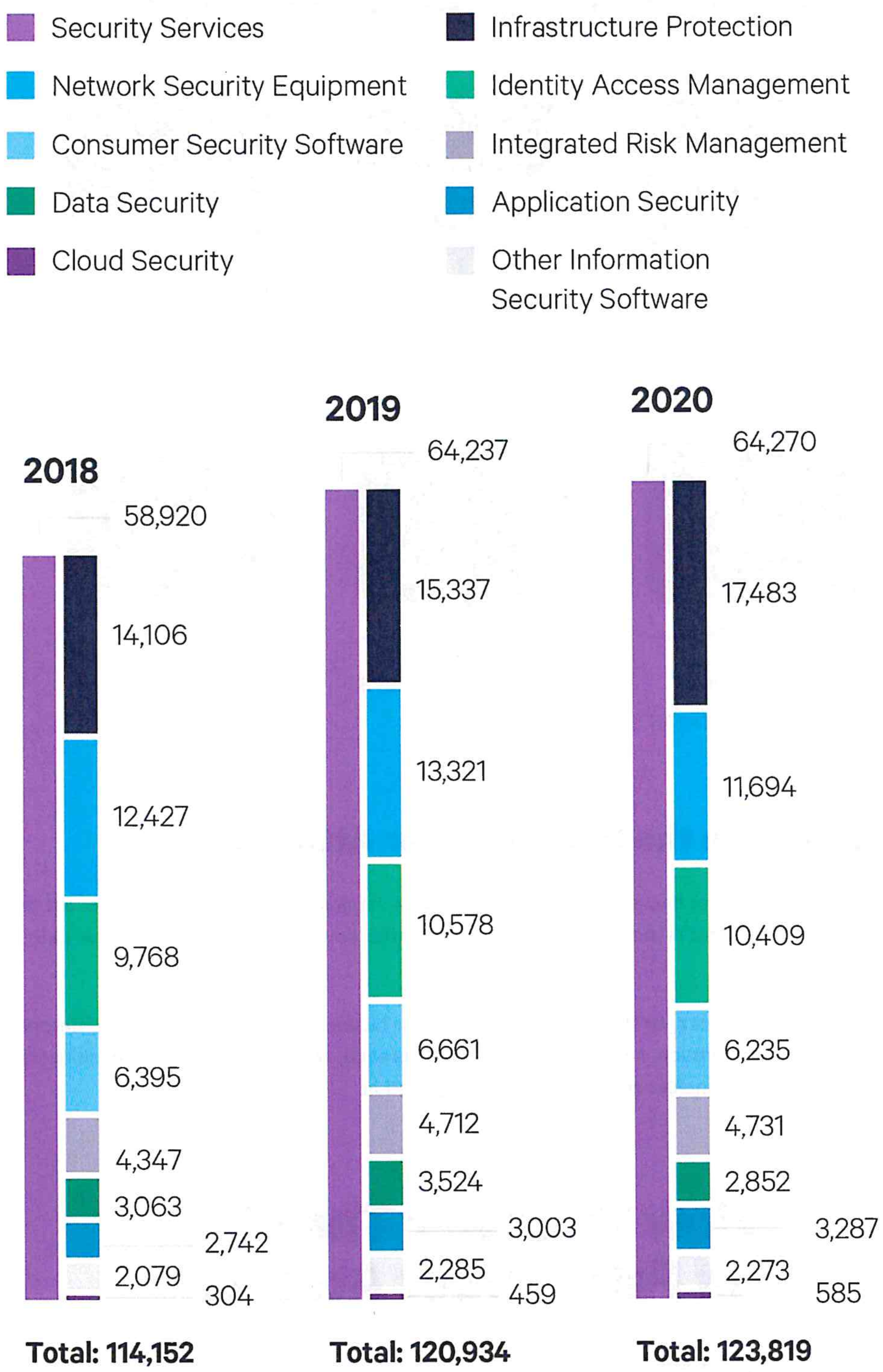
71% expect cybersecurity budgets to increase **in the next three years**.

Global Security Spending

Let's take a look at how cybersecurity spending has grown around the globe — broken down by product or service.

Worldwide Security Spending by Segment, 2018-2020

(Millions of U.S. Dollars)

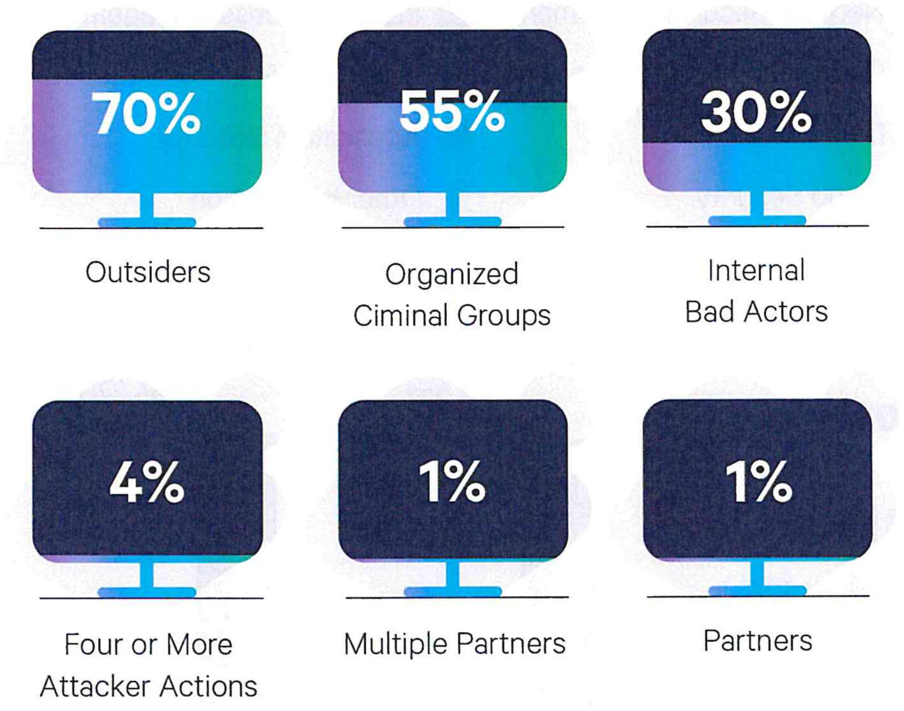


Who's Behind Data Breaches?

The average person might assume the files on a company database are a bunch of boring documents, but hackers know the hard truth about that hard drive.

According to Verizon's Data Breach Investigations Report, the majority of cyber attacks are triggered by outsiders, insiders, company partners, organized crime groups, and affiliated groups. We break down the percentages of each:

Who's Behind Data Breaches?

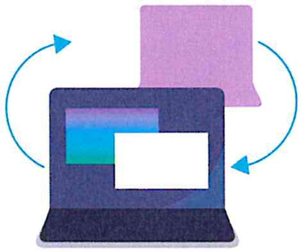


How to Reduce the Risk of Cyber Attacks

With the increasing threats of hackers mishandling your data, implementing processes to prevent data security breaches is the most responsible course of action after having adequate professional data breach insurance.

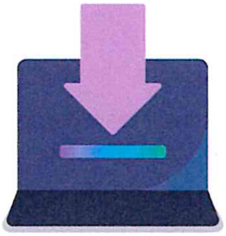
Data breach laws vary by state, so depending on where your business is located, there are different factors to take into consideration. Notifications around the breach, what's covered, and penalties will look different depending on the incidence and state you're located in.

How To Lower The Risk of Fatal Cyber Attacks



Reduce Data Transfers

Keep sensitive data on personal d



Download Carefully

Verify sources and avoid unnecessary downloads.

Improve Your Passwords

Use a string of symbols with no meaning and regularly update.

Update Your Software

Regularly install the latest updates on your devices.

Monitor for Data Leaks

Quickly detect, respond, and stop any activity with software.

Develop a Breach Response Plan

Establish a formal plan to manage and contain potential damage.

1. Reduce Data Transfers

Transferring data between business and personal devices is often inevitable as a result of the increasing amount of employees who work remotely. Keeping sensitive data on personal devices significantly increases vulnerability to cyber attacks.

2. Download Carefully

Downloading files from unverified sources can expose your systems and devices to security risks. It's important to only download files from sources and avoid unnecessary downloads to lower your device susceptibility from malware.

3. Improve Password Security

Password strength is the first line of defense against a variety of attacks. Using strings of symbols that don't have a meaning, regular password changes and never writing them down or sharing them is a crucial step to protecting your sensitive data.

4. Update Device Software

Software providers work hard on continuously making their software more secure, and regularly installing the latest updates will make your devices less vulnerable to attacks.

5. Monitor for Data Leaks

Regularly monitoring your data and identifying existing leaks will help mitigate the potential fallout from long-term data leakage. Data breach monitoring tools actively monitor and alert you of suspicious activity.

6. Develop a Breach Response Plan

Data breaches can happen to even the most careful and disciplined companies. Establishing a formal plan to manage potential data breach incidents, primary cyber attack response plan, and cyber attack recovery plan will help organizations of any size respond to actual attacks and contain their potential damage.

It's clear that businesses are under a constant threat of cybercrime and must take steps to defend their data. Don't wait until it's too late, take steps today to prevent future data breaches and the consequences that follow. Akin to the need for having adequate cyber liability insurance, having adequate data protection is essential.

Sources: Cybersecurity Ventures 1, 2 | IBM | Ponemon | Statista | Verizon | World Economic Forum

First name*

Last name*

Email address*

Company name*

Download

Related Articles

BLOG RISK MANAGEMENT

BLOG INSURANCE EXPLAINED

Have any questions? We got you covered. 😉