FORTRESS
SECURITY RISK MANAGEMENT
A Division of MCPc

Worksheet

Cyber Attack Cost Worksheet

Cyber resliency is business resiliency.

If you are worried about cybercrime and want to sleep better at night, are looking for a co-managed solution to enhance your teams capability and capacity, or are simply seeking a second opinion, Fortress stands ready to help protect your organization from the ravages of cybercrime.

IN CASE OF EMERGENCY:

Cyber Attack Hotline: 888-207-0123
Report an Attack: IR911.com

FOR PREVENTATIVE & EMERGENCY RESOURCES:

RansomwareClock.org

Every business is different. Doesn't matter if you're big or small, you're a target. Cybercriminals may be after your "IP" or your "secret sauce" process, or maybe, just after your money. Cybercrime has become the world's most profitable business. Some businesses are targeted by nation states, but the great majority are targeted by very efficient criminal enterprises with a corporate structure not unlike most American businesses. The typical attacks employ business email compromise or ransomware simply to separate you from your money. Because anyone with money is a target.

SCARY BUT TRUE STATS

- Every **11 seconds** a new ransomware attack hits this year.
- The average ransomware payment is **~$300k, up 45%** from a year ago.
- Ransom payments account for only **10%-15% of the total cost** of an incident.
- **207 days** is the average time to identify a breach. Meaning the bad guys are in your system for over 6-months.
- **21 days** is the average downtime caused by a ransomware attack.
- **93%** consider an organization's trustworthiness prior to purchasing.
- **59%** would avoid doing business with a company cyberattacked in the past 12 months.
- **Only 21%** of security professionals think their current security controls are adequate.

See Next Page for Worksheet >

COST CENTER

Downtime & Business Loss

- **Average downtime: 21 days**

How long can your business "Hold its breath?"	Days to recover:	
What's your daily cash burn?	Daily cash burn:	
Loss per cyber attack outage	$:	

Lost Business, Lost Contracts, Lost Clients

- **$1.52M average cost of lost business**

Consider the long term value of your best customers.		
Additional acquisition time and cost to replace them.	$:	

Legal & Litigation:

- **Cyber legal fees in 2022 average $375-$425/hour**
- **Legal fees are ~8%-10% of the demand.**

Will outside legal counsel be required?	Y/N:	
Will customers sue over non-delivery or broken contracts?	$ Loss:	
Will you have to defend separate civil lawsuits?	Y/N:	

Reputation & Brand Damage

- **59% would avoid doing business with a company cyber attacked in the past 12 months.**

How long will the stigma of breach stay with your company?	Duration:	
Will you need to hire a crisis communications or PR firm?	Y/N:	
Will additional sales and marketing be required to replace lost customers?	PR + Marketing $:	

Employee Morale & Recruitment

- **31% led to employee layoffs, including C-level.**

Will attack expenses force staff reductions?	Staff Reduction:	%
Will hiring new talent be more difficult and slower?	Retention $:	
Will you lose employees dues to credibility?	Y/N:	

Vendors & Partners

- **58% believe they have suffered a vendor related breach.**
- **63% have no vendor related safeguards.**

Will existing partners terminate their relationship with your company?	Y/N:	
Will suppliers require shortened payment terms impacting your cash flow?	Y/N:	
Can you quickly replace existing vendors with new ones?	Y/N:	

COST CENTER CONT.

IR, Recovery & Remediation, Security Software & Services

- **Ransom payments account for only 10%-15% of the total cost of an incident.**
- **Over 60% of ransomware victims don't fully clean out the virus payloads cybercriminals strategically leave behind and are attacked again by the same gang within 9-months.**

Additional costs for an incident response team, recovery of data, and the rebuilding of systems.	IR Project Cost $:
	New Monthly Security Fees $:

Financial & Insurance Issues

- **Cyber insurance premiums continue to rise particularly for those companies with less than excellent cyber controls.**

Will your business insurance premiums go up? If so, by how much?	Insurance Increases $:
Loss of insurance after breach?	Y/N:
Should you add cyber insurance to your risk management strategy?	Cyber Insurance $:

Investors & Shareholders

- **110 days after a breach, a company hits a low point.**
- **3-years later share prices continue to fall an average of 15.6%.**

Will you be able to sell your company at the valuation you desire? **Cyber due diligence concerns may cause a price adjustment downwards of up to 15% of the purchase price*	Y/N:
Will investors (private or public) divest ownership?	Divestments $:
Will sell-offs impact market cap?	Market Cap Loss $:
Will acquiring new investors become much more difficult?	Y/N:

Regulatory Fees, Notifications & Mailings, Credit Monitoring

- **All 50 states have breach notification laws.**
- **66% of companies see compliance mandates driving spending.**
- **If PII data is exfiltrated, a year of credit monitoring may be required (some states require multiple years) @ $9-$40/mo. per person**

Will you be fined for failing to protect customer data?	Y/N:
Do you know cost-per-record fines for violated statutes?	Fines $:
Does your industry and/or state regulations require customer notifications be sent?	State Law Fees $:
Are you required to provide credit monitoring to affected customers?	Y/N:
If so, for how long and at what cost per person?	# of records x $9 x 12 months:

In the cyber risk world, an ounce of prevention is worth a ton of cure.

TOTAL $: _____

FULL-SPECTRUM CYBERSECURITY

Security Consulting

Assessments

- Framework Assessments
- M&A Cyber Due Diligence
- 3rd Party Vendor Risk
- Technical Testing
  - Penetration Tests
  - Vulnerability Scans
- Regulatory Compliance

Program Development

- Virtual CISO
- Multi-Factor Authentication
- GRC Advisory
- Identity & Access Management
- Threat Management
- Training / Phishing Tests

Incident Response Preparedness

Managed Security

Managed Services

- Cybersecurity-as-a-Service
- Guardian Managed Patching
- Sentinel Endpoint Detection & Response (EDR)
- VantagePoint Managed SIEM
- Vault Managed Backup
- Frontline Help Desk

* Monitoring & Management via wholly owned 24/7/365 U.S. Security Operations Centers

Incident Response

Full Service-IR

- Contain & Control
- Assess & Analyze Attack Impact
- Threat Elimination & Disaster Recovery
- Digital Forensics & Investigation
- Litigation Support
- Remediation Services
- Crisis Project Management
- Post Incident Assessment & Improvement Roadmap

ABOUT FORTRESS

Fortress Security Risk Management protects companies from the financial, operational, and emotional ravages of cybercrime by enhancing the performance of their people, processes, and technology.

Offering a robust co-managed solution to enhance an internal IT team's capability and capacity, Fortress features a full suite of managed security services (SOC, patching, EDR, backups) plus specialized services like Cybersecurity-as-a-Service, Incident Response including disaster recovery & remediation, M&A cyber due diligence, GRC advisory, identity & access management, threat management, vulnerability assessments, and technical testing. With headquarters in Cleveland, Fortress supports companies with both domestic and international operations.

IN CASE OF EMERGENCY:

Cyber Attack Hotline: 888-207-0123

Report an Attack: IR911.com

FOR PREVENTATIVE & EMERGENCY RESOURCES:

RansomwareClock.org