NetStandard
Managing Technology

Cyber Incident Quick Reaction Sheet

The world of business continuity, disaster recovery, and incident response can be confusing and the lines among required plans can be blurry. As a business owner or operator, you must decide how much time and energy to invest in a strategy for continuity in the event of any type of emergency.

In the event of a cybersecurity incident, defined as an identified compromise or threat that causes the interruption or serious degradation to a technology service, data or application, you want to have a plan for survival. Creating a simple response checklist will help coordinate your team's response in a crisis and can ensure you have the right information at your fingertips.

This checklist is intended to be a quick reference guide for leadership in response to a cybersecurity incident. It is not comprehensive. It will need to be customized for your business, your systems, your vulnerabilities. But it will help you to think through the information you need in the event of an emergency, and may trigger conversation around bigger topics, such as business continuity strategy or overall cybersecurity preparedness, that will enable you to think proactively about risk and response.

Emergency Contacts

Use the below as a central place to store useful contact information that you'll need if an incident is declared. Can note who has the authority to declare the incident, and who will be responsible for coordinating internal and external communications. The backup person should be used in case the primary is unavailable due to the cause of the incident or other circumstances.

Title	Company	Contact Information	Backup Contact Information
Internal Incident Response Team	[Internal -- CISO / CIO / CTO / …]		
	[Internal -- Security]		
	[Internal -- IT]		
	[Internal -- Privacy]		
	[Internal – General Counsel]		
	[Internal – Operations]		
	[Internal -- Communications]		
	[Internal – CFO]		
	[Internal -- HR Member]		
IT MSP Provider	*NetStandard*	*913-428-4200 24x7 NOC NetStandard*	*xxx-xxx-xxxx NetStandard CTO Mobile*
MSSP/SOC Provider	*NetStandard*	*913-428-4200 24x7 NOC NetStandard*	*xxx-xxx-xxxx NetStandard CTO Mobile*
Breach Counsel			
Cybersecurity/Cyber Forensics Vendor			
Decryption/Negotiation Vendor			
Federal Reporting agencies for Cyber Crime	FBI Field Office Cyber Task Forces	http://www.fbi.gov/contact-us/field	
	Internet Crime Complaint Center	http://www.ic3.gov	
Breach Notification Vendor			
eDiscovery Firm			
Payment Card Processor and Processor Agreement location			
Telecommunications Vendors			
Data Center Vendor			

Backup Service Provider			
Public Relations team			

Cyber Security Insurance Policy Information

In most instances, cybersecurity insurance is recommended for any business that stores confidential or proprietary information. As cyberattacks have increased over the last few years, even small businesses are encouraged to evaluate insurance as a way of mitigating the risk of data loss or compromise from a cyberattack. Prerequisites for cyberinsurance are also on the rise, and in most cases businesses will have to meet minimum established security standards before they are able to be insured.

Make sure prior to an incident that you understand the types of coverages you have that may provide assistance, and how specifically you'll engage your cyberinsurer in the event of an incident. Many cybersecurity incidents occur on weekends or holidays, and therefore it's important to understand how to engage to optimize response.

Your cyber Insurance company will dictate which vendors you engage as a part of your response, and depending up on the size and coverage in the policy, the vendors chosen may determine your options for reporting and response. We recommend having your insurance provider pre-approve your response team as a part of policy creation or renewal, so that you are prepared to engage quickly.

Cyber Insurance Carrier:	
Cyber Insurance Contact Number:	
Cyber Insurance Policy Number:	
Cyber Insurance Coverage Effective Dates:	
Cyber Insurance Policy Document Location:	
Cyber Insurance Broker Contact Info:	
Internal Insurance SME Contact Info:	

Emergency Systems, applications:
For each system you use in the business, think about what types of data is stored, how critical the information is (either as priority order, ranking, or workaround capacity), the contact information for your Subject Matter Experts (SMEs) on that application, and what you might do in the event the system is unavailable. We've started you off by listing some typical data types, and potential answers, but most organizations use a variety of tools in each space that will need to be listed.

Business Application	Usage/data	Criticality	Contact/Expert	Workaround
Email: *Office 365*	*Internal/external communications; email addresses, phone numbers, account numbers*	*Medium*	*NetStandard, 913-428-4200*	*Customer call tree, phone/Slack, Personal employee directory*
Accounting: *hosted GP*	*Financials, account numbers, invoicing*	*High*	*Zack Morris, 999-999-9999*	*Monthly reports, ERP system, offline backups*
Banking:				
ERP system:				
Collaboration (voice, conferencing, chat)				
Knowledge Base:				
Facilities/Physical Security:				

Backup Systems

Knowing the location and key contact information about your backup providers is essential during a cybersecurity incident. For each of your business applications, document the location, frequency and schedule for your backups, as well as whether there is an offline or immutable copy available.

Business Application	Data Types	Primary Backup	Contact/Expert	Offline Copy?
Email: *Office 365*	*Internal/external communications; email addresses, phone numbers, account numbers*	*SAAS*	*NetStandard, 913-428-4200*	*Yes, DataSafe*
Accounting: *hosted GP*				
Banking:				
ERP system:				
Collaboration (voice, conferencing, chat)				
Knowledge Base:				
Facilities/Physical Security:				