Cyber Breach Checklist:

What Every Business Should Know to Prevent and Handle a Cyber Security Breach

Contents

1

Part One: Protecting Your Business

- What is Cyber Security?
- What is Your Threat Landscape?

2-4

Part Two: About Your Business

- What Kind of Data do You Have in Your Business?
- How is Your Data Protected?
- Who Has Access to Your Data?
- What is at Risk?
- Cyber Security Checklist

Part One - Protecting Your Business

A data breach is a business owner's worst nightmare. It comes to life when an incident occurs where sensitive or confidential data has been accessed in an unauthorized way. Criminals are coming up with complex, and modern, tactics to sneak their way into computer systems. The last thing a business owner needs is their business becoming headline news and suffering financial damage because their client's data was stolen.

What is Cyber Security?

Since modern businesses use technology to run their everyday operations, it is crucial to protect these indispensable computer systems.

Physical protection, yes, but also protection from online threats. Hackers are becoming increasingly clever with the ways they can access confidential data. Malware through email scams, gaining access to secure networks, and unauthorized downloads are just a few ways that a cyber breach can happen.

A second component to cyber security is the human beings who use the computer systems. Human errors are unavoidable but if employees are aware of the warning signs, it can strengthen cyber security habits within the organization.

What is Your Threat Landscape?

Each industry will have a different classification of threats and criminals trying to gain access to their information. The threat landscape, the outlook for severity and intensity of attempted hacks, is only getting worse across all industries.

"By any measure you want to use, the trend line is going the wrong way," said Rob Joyce, White House cybersecurity coordinator. "Whether you look at breaches, whether you look at criminal activity...we've got to worry."

Data Breach Case Study #1 - Volunteer Voyages

Dr. David Krier, the singular owner of a small travel business, lost over $14,000 when fraudulent withdrawals were taken from his business bank account. While the Dr. was travelling abroad, the company's debit card number was stolen over the internet and when he returned home he noticed the missing funds. Unfortunately for him, the bank was not able to recover the the money.

Part Two - About Your Business

What Kind of Data do You Have in Your Business?

Generally a business has all different kinds of data. Some pieces of data are more valuable than others, but all data is of value to someone.

Types of data you may have:

Customer Data

- Names
- Addresses
- Financial information
- Emails
- Home address
- Buying habits/history

Employee Data

- Social Security Numbers
- Payroll files
- Direct deposit information
- Work and personal email addresses
- Phone numbers

Company Data

- Financial records
- Marketing plans
- Product designs
- Tax information

Data Breach Case Study #2 - Patco Construction

A construction company in Tennessee was hit with a Trojan malware that allowed cyber criminals to steal more than $327,000 from the company. The scary part of a Trojan virus is that it is easily undetected. It allows cyber criminals to spy, steal data, and even gain backdoor access to systems. The company was able to recover a small portion of the stolen money but they suffered a major financial setback.

How is Your Data Protected?

In an ideal world, your data would live on one computer system that is safely secured without the data travelling through the network to various employees. But that isn't the case.

For data to be used in a meaningful way, it must be available to employees for analytical and research purposes, contacting customers, and marketing projects. There are risks that come with "travelling data."

Business owners should have a plan in place that includes policies and procedures for how different types of data are handled, stored, and protected.

Who Has Access to Your Data?

Not all of your employees need access to all of the company's data. For example, Diane from Marketing doesn't need access to payroll data.

Data inventory means that you have a record of all company data, where it is stored, level of clearance required to access, and who has access.

What is at Risk?

The danger of a breach puts many things at risk for your business. Money, customer trust, investors, sensitive data, reputation, and IT equipment are all assets that can be compromised by a data breach.

Data Breach Case Study #3 - Menlo Park Dental Office

This dental practice was the victim of a ransomware attack that exposed the confidential information of its patients. The hackers were able to access email addresses, full names, home addresses, dates of birth, Social Security Numbers, and dental treatments. The virus went undetected for over two weeks but once discovered, the authorities were contacted and all patients were notified of the incident and what action was being taken to make sure this never happens again.

Cyber Security Checklist

Having a plan in place of what to do before, during, and after a data breach can save you from an expensive headache.

Before

- [ ] Develop a full set of cyber security policies and procedures
- [ ] Create strong and unique passwords
- [ ] Form a Security Team to manage your cyber security program
- [ ] Provide cyber security awareness training to all employees

During

- [ ] Mobilize the incident response team
- [ ] Ensure systems and business continuity
- [ ] Create a full incident report
- [ ] Contact all affected third parties

After

- [ ] Review the incident report and make sure proper procedures were followed
- [ ] Determine what changes (if any) need to be made in order to avoid future breaches
- [ ] Determine any possible financial or reputational damage caused by the breach
- [ ] Report incident to proper authorities when applicable

This only scratches the surface for what your cyber security habits should look like. For additional resources and information, visit http://www.securicy.com.