

Essential Business Cyber Security Tips

Protecting Your Business From Cybercriminals

cipher
a PROSEGUR company

Table of Contents

1. Introduction — Cyber Security is Everyone's Business
2. Riskiest Threats to Businesses Today
3. Security 101 Checklist
4. Network Security Essentials
5. Traditional vs. Next-Gen Anti-Virus
6. Privacy and Data Security Essentials
7. Email Security Essentials
8. Avoiding Scams, Fraud, & Hoaxes
9. Planning for Security Incidents

cipher
a PROSEGUR company

Introduction



CYBER SECURITY IS A SHARED RESPONSIBILITY

It's a simple fact that cyber security affects all of us. If just one computer is hacked, it can lead to millions of compromised accounts. Everyone has a responsibility in building a culture of cyber security. We all need to work toward improving online safety and security for future generations.

To create a culture of cyber security, you make cyber security a part of the DNA of your organization. Creating a culture of cyber security means that if you see something off or strange, you say something. It also means establishing a culture where we're all concerned, and you know who to contact when there's a problem.

There are three critical areas when creating a culture of cyber security as a shared responsibility.

1

Implementing Basic Cyber Security Best Practices & Policies

2

Protecting Your Data a.k.a "The Crown Jewels"

3

Educating Your Employees on Cyber Security Best Practices

Cyber Security is a Shared Responsibility

1 Implementing Basic Cyber Security Best Practices & Policies

Shared responsibility starts with building cyber security best practices and basic business policies for security. You must develop policies and standards that make it harder for criminals to obtain your valuable data assets. This is the first step toward building a culture of cyber security.

2 Protecting Your Data a.k.a “The Crown Jewels”

Whether personally or professionally, we all need to be focused on protecting our data. It means not placing your Personal Identifiable Information on social media networks. And from a professional perspective, it means protecting your company’s critical data assets from risky security situations. It’s your employees’ duty and shared responsibility to safeguard any vital data they touch. Your employees and leadership need to know the security processes needed to protect their assets and the business.

3 Educating Your Employees on Cyber Security Best Practices

Solidifying a culture of cyber security begins with education and awareness. Most people want to comply with Security Policies, they just need to know what they are and the rationale that supports them. User awareness is a key ingredient, one that many would say is the cornerstone of any security program.

Riskiest Threats to Organizations Today



- Phishing: A social engineering scheme used to obtain sensitive information such as usernames, passwords, and credit card details



- Ransomware: The hacker leverages malware but requests a ransom to “unlock” an organization’s files and data



- Malware: Software designed to interfere and wreak havoc on a system (common names – virus, spyware, worms, and Trojans)



- Insider Threats: Employees within your organization may pose a significant threat to your organization

Riskiest Threats to Organizations Today



- Web Application: Web application attacks occur through code injections on a website, creating pop-up screens that ask for personal information



- Distributed Denial-of-Service Attacks (DDoS): Malicious streams of traffic, often using botnets, aimed at shutting down a website or cause slow performance and public embarrassment

- IoT Security Vulnerabilities & Botnets: The rapid pace of innovation and demand for consumer IoT devices leads to botnets leveraging malware to take advantage of unprotected, connected devices and then create an army of bots by using these vulnerabilities



- No-Tech Hacking: Cybercriminals use many tactics, including tailgating, shoulder surfing, and dumpster diving to steal sensitive information. Physical security is often an overlooked as an aspect of information security

Security 101 Checklist

Below are some essential steps you can “check off” to improve your security operations. We will go into more detail with these later throughout the eBook.

1. Everyone filters inbound traffic from the Internet with firewalls. Only allow inbound traffic to a DMZ, and only allow traffic needed by the business.
2. Use a 3rd party hosted email. If you must have things like RODC or Sharepoint in a DMZ, segregate them and don't allow inbound traffic from them -- and make sure they're patched.
3. Filter outbound network traffic to only allow traffic needed by the business.
4. Patch your operating systems, software, and firmware. You may want to consider a centralized patch-management system.
5. Use Group Policy or other mechanisms to control how removable media can be used.
6. Backup your data and applications regularly. Test and confirm the backup process is working properly on a regular basis as well.
7. Use Next-Generation Antivirus and Endpoint Protection Solutions like Carbon Black. Go for 24x7 coverage using Managed Services.
8. Use IPS on your perimeters and protect internal segments that house sensitive data, such as accounting and HR systems. Outsourcing functions that involve sensitive data to cloud services is a cost-effective.

Security 101 Checklist



9 Use the principle of “least privilege” to manage accounts. No users should have administrative access unless absolutely necessary. The user’s privileges should be based on what access they need to specific files.

10 Only use third parties that have security certifications such as SOC2 and ISO 27001.

11 Block all ads. Ransomware is frequently distributed through malicious ads served when visiting certain sites. Blocking ads or preventing access to certain sites can reduce infection from these malvertising campaigns.

12 Use a third party to conduct phishing simulations and training. Track your results over time.

13 Categorize and inventory your data and assets based on organization value. Then, create a risk category for each of these data assets for each organization unit.

14 Conduct and require security training for your users on an ongoing basis. Establish expectations for secure behavior. The cornerstone of every security program should be user awareness.

15 Enhance your abilities to detect, notify, and respond -- the best way is to use Managed Security Services.


Network
Security
Essentials
cipher
a PROSEGUR company

Patch Your Systems Regularly

Successful ransomware attacks like WannaCry, Petya, Locky, and Bad Rabbit target and exploit vulnerabilities in your operating system and software applications. Malware such as these recent incidents will spread like a worm, exploiting a Windows SMB vulnerability rather than using methods such as phishing or drive-by attacks (often instigated by compromised ad networks advertising on the page).

Hundreds of patches are released every month by software distributors. In fact, on average, research points to more than 60 vulnerabilities per day in 2017 and that number is rising quickly. However, the process of patching hundreds of machines becomes increasingly complex if done manually: it doesn't scale well. Nonetheless, and not specific to ransomware, it's critically important to keep your systems up-to-patch to manage vulnerabilities.

A solid patch management system starts with a comprehensive discovery and inventory of your systems using tools to automate the process. You should devise your own patch management strategy and plan for managing patches and upgrades or employ the consulting services of an expert security consultant that can help you handle these changes. A comprehensive security strategy will include automated software patches and eliminates the potential for cybercriminals to exploit your software and OS vulnerabilities.

Many IT organizations are reluctant to setup automatic patching due to concerns about side effects and unexpected impacts of so doing. It's not worth the worry for most organizations – it's more advisable to setup everything to auto-update, including operating systems, and deal with unexpected impacts as they arise!

Install Endpoint Protection

Data breaches put a major focus on endpoint protection. Sensitive documents now need to be created and shared in and outside the office. Therefore, endpoint protection is a must have for your organization. Anti-virus is just not enough to prevent a major attack. In fact, if you rely just on anti-virus protection you will leave your endpoints, like desktops and laptops, exposed. Your desktops and laptops can become a major gateway for breaches if they are left unencrypted.

A comprehensive endpoint protection solution will use encryption to prevent data loss and leakage, enforce unified data protection policies across all your servers, networks, and endpoints, thereby reducing the risk of a data breach.
A comprehensive endpoint protection solution will use encryption to prevent data loss and leakage, enforce unified data protection policies across all your servers, networks, and endpoints, thereby reducing the risk of a data breach.

Endpoint protection such as Next-Gen Malware Protection (Carbon Black, Cylance, Crowdstrike) provides superior performance over older anti-virus application methods.

Cyber Tips

- Inspect all network traffic
- Classify it as benign, malicious, or questionable
- Analyze questionable traffic rapidly to determine whether it is malicious or not
- Curtail any malicious traffic
- Take the necessary steps to remediate any damage

Encryption Methods

Whole disk encryption protects the enterprise from lost or stolen laptops. When the user logs in data on the drive is accessible in an unencrypted manner, but if lost or stolen, unless the laptop can be logged into, the disk encryption protects the data – if a hard drive is attached to another PC, the data cannot be accessed.

Encrypted Data (at rest, in transit, & in use)

- Data at Rest: encrypt data in the database; field encryption is preferable, table and database are also options
- Data in Transit: encrypt both the data and use an encrypted transport protocol such as SSL or VPN
- Data in Use: sensitive data should be obfuscated, such as showing dots for a credit card number (except possibly the last 4 digits)

Vulnerability & Compliance Management

Using a vulnerability and compliance management (VCM) tool or at the very least completing a vulnerability assessment will help you identify the gaps, weaknesses, and security misconfigurations within your physical and virtual environments. VCM can continuously monitor your infrastructure and IT assets for vulnerabilities and compliance weaknesses and configuration best practices.

Some of the benefits that will help mitigate a data breach include allowing your security team to better understand the security vulnerability risks of the environment, i.e. threat landscape, and priorities around what requires remediation. A good VCM will allow you to create an action plan to remediate these vulnerabilities and assign them to appropriate staff members.

Cyber Tips

Penetration tests and vulnerability assessments performed to understand gaps or potential threat areas are quite eye-opening. Some organizations may want to leverage ethical hacking to test behavior and potential exposure.

Regular Audits on Security Posture

Completing regular security audits to identify potential new gaps in compliance or governance will help in validating your security posture. A security audit will be a more thorough assessment of your security policies compared to the vulnerability assessment or penetration testing. A security audit considers the dynamic nature of the organization as well as how the organization handles information security.

Common questions that may come up in the security audit could include:

1. Does your organization have documented information security policies?
2. Do you have a management process in place, escalation profiles, and procedures documented and tracked, a playbook in place in the event of incidents or breaches?
3. Do you have network security mechanisms in place (next-gen firewalls, IDS/IPS, EPP, etc.)?
4. Do you have security and log monitoring setup?
5. Are there encryption and password policies?
6. Is there a Disaster Recovery & Business Continuity Plan?
7. Are applications tested for security flaws?
8. Is there a change management process in place at every level within the IT environment?
9. How are files and media backed up? Who will be able to access this backup? Are restore procedures tested?
10. Are the auditing logs reviewed? When are the security auditing logs reviewed?




Traditional
vs.
Next-Gen Anti-Virus
cipher
a PROSEGUR company

What is Next-Gen Antivirus?

Traditional antivirus programs have been the primary means of protecting endpoints since the late 1980s, where digital threats are detected through signature databases that allow infected files to be recognized and cleaned with vaccines.

This type of antivirus has lost its effectiveness as operating systems, software, computer networks and digital threats have become more sophisticated over time. The rapid growth in the number of threats is continuous and includes new malware as well as variations of the same family, which makes a signature-based approach ineffective because it cannot keep up with the growth in a timely manner.

The way traditional antivirus also works dramatically damages the endpoint's performance by its intrusive behavior. Performing periodic disk and computer memory scans and frequent subscription updates consume hardware and network bandwidth when they do not require system-wide reboots, which causes user dissatisfaction.

The next generation antivirus (NGAV) differs from traditional antivirus solutions by incorporating many extra features, such as the ability to learn the behavior of the endpoint in which the solution is installed, identifying any anomalous behavior without querying a signature database or vaccines. Improved environment analysis and unknown threat detection techniques also enable greater efficiency without consuming computing power or requiring frequent update downloads.

In addition to its focus on digital threat prevention, NGAV also protects the system against zero-day exploits (wherever it is written in the case of files with PDF, DOC, and DOCX extensions, as well as executables) to handle malicious code and infect the endpoint. Subscription-based antivirus does not easily detect this type of attack.


Privacy
&
Data Security
Essentials
cipher
a PROSEGUR company

IT Asset Inventory & Categorization

An inventory of what hardware and software assets you have in your network and physical infrastructure will help you gain a greater understanding of your organization's security posture. An asset inventory can also be used to build categories and ratings around the threats and vulnerabilities your assets may encounter. Categories and ratings for these vulnerabilities can help you better prioritize the remediation efforts that will take place on these assets.

Below are some of the common inventory questions you can use to assess your IT inventory:

Systems & Hardware:
What endpoints (PCs, laptops, mobile devices, printers, etc.) are used within the organization?

Networking:
Is the organization using a wired (LAN) or wireless network? Is it secured and how? Is there a guest network? Who has the wireless password? How frequently is this password updated?

Application & Data:
What applications does your organization currently use? What applications do any third parties manage?

Users:
Who are the users in your org that have access to systems? What are their privileges?

Create Your Security Programs & Policies

Security programs should include measures to prevent a data breach. The security policies you create will consider how you identify, protect, detect, respond, and recover from data breaches and security incidents. Security programs should cover each of these areas in their entirety.

A critical early step in creating an information security program is identifying who will be responsible security identification, protection, detection, response, and recovery. The security policy should designate either one individual or several individuals or third parties responsible for coordinating the security posture of the organization. It should also define the responsibility each employee has with security within the organization – from CEO to support staff.

A robust security policy will set the tone for any security incidents affecting the organization. The security policy should specify the following:

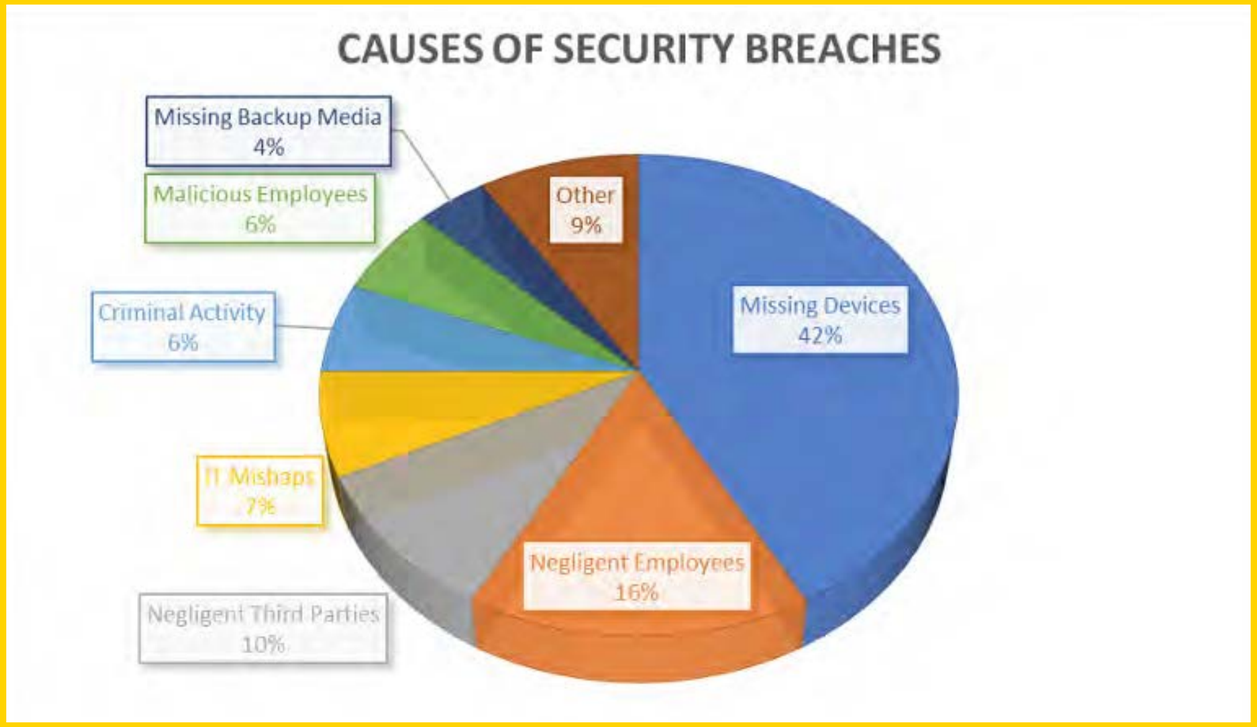
- Acceptable file sharing methods
- Internet usage guidelines
- Proper use of wireless devices
- Proper use of encrypted technologies
- Password policies
- Prohibited applications
- Prohibited services
- Privacy Policy
- Backup policies
- Acceptable remote access
- How to properly dispose of data (sensitive and non-sensitive)
- Spam & Policies

Create a Data Loss Prevention (DLP) Strategy

DLP in its simplest terms is a security strategy to prevent or protect users from sending sensitive information or critical information outside the corporate network. It can also be used to describe various security technologies and tools used to prevent insider threats from leaking or sending corporate files to cloud storage, personal emails, social media sites, or other unauthorized locations.

DLP monitors and safeguards your data in transit , data at rest , and data in use .

DLP security tools should watch for unauthorized attempts to access or store data. When the user logs in the to the device, data on the drive is accessible in an unencrypted manner, but if lost or stolen, unless the laptop can be logged into, the disk encryption protects the data – if a hard drive is attached to another PC, the data cannot be accessed.



The Ponemon Institute found that 85% of companies around the world have experienced some form of data loss in the last 24 months. Most of these data loss incidents occur from within the organization (See Figure 1).



Email Security Essentials

cipher
a PROSEGUR company

Email Security Tips



Organizations use email every day. It's a fundamental tool for the business. However, cybercriminals use email as the primary method for spreading viruses and malware and most commonly used to compromise organizations. Below are a few tips for your email security.

- Sensitive or confidential information should typically not be sent via email. If it needs to be sent via email, you should use encryption to ensure that the sensitive information is not compromised.
- Avoid any phishing attempts by not clicking suspicious links, checking the links to verify the URL, and reporting suspicious emails as SPAM.
- Check your email service providers SPAM filters to ensure that the filters are set to filter the right content.
- Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. Email filters ensure that automatic updates are enabled on your email application, email filter and anti-virus programs.
- Companies should document how they handle email retention and implement basic controls in attaining those standards. Certain industries have specific rules that specify how long emails can or should be retained. The basic rule of thumb is only keep it as long as it supports your business efforts. Many companies implement a 60-90 day retention standard.
- Policies are important for setting expectations with your employee and ensuring adherence to your published polices. Any policy should easy to understand and enforce. Some critical areas to address within an email policy include what the company email system is used for and what data can be transmitted and received. Other areas of the email policy should include email retention, privacy and acceptable use.

Phishing Protection



There are ways to prevent spammers and phishers from spoofing your domain in the FROM: addresses of email they send: Sender Policy Framework (SPF), DomainKeys Identified Email (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). Optimally, all three should be used in concert for phishing protection. They are very easy to configure, and everyone should do so.

Sender Policy Framework (SPF)

SPF was first published as an experimental RFP in 2006 after about six years of discussion and debate. It defines what email gateways (Mail Transport Agents, or MTA's) are allowed to send email for a domain. The definition for these resides in an external DNS, such as a Linux server running Berkeley Internet Name Daemon (BIND). BIND servers are configured with zone files that return either IP Addresses when queried with a server name (record types A or CNAME), Server Names when queried with an IP address (record type PTR), or in this case, information in the form of TXT records.

example.net. IN TXT "v=spf1 mx a:pluto.example.net include:aspmx.googlemail.com -all"

The DNS zone record above says that for email addresses from the example.net domain, MX (mail exchanges) that send email are named either pluto.example.net or aspmx.googlemail.com, with all other server names not authorized. If an email with FROM address that includes example.net came from any other email gateway, it is not to be trusted – it could be spoofed. The receiving email gateway checks this by looking at the example.net's SPF record in DNS. Many companies require SPF be configured for your domain in order for your email to be successfully delivered to them.

Phishing Protection

DomainKeys Identified Email (DKIM)

DKIM dates back to 2004, a merger of Yahoo's "enhanced DomainKeys" and Cisco's "Identified Internet Email." DKIM involves asymmetric public key cryptography, i.e., a generated public and private key. The public key is included in a TXT record along with some other bits of information; the sending email gateway(s) are configured with the private key to include in headers of the email to be sent. The keys are generated in a variety of ways, including free public sites.

Here's an example of an email header containing DKIM information. Based on this, the receiving gateway will check example.net's DNS for the corresponding public key.

DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=itverx.com.ve; s=example; t=1342650894;
bh=pFo6ZYCLWFoBWmva8IlsxprN/QOinqGTGscl1MBI3sQ=; h=MIME-Version:Sender:In-Reply-To:References:Date:Message-ID:
Subject:From:To:Cc:Content-Type; b=Fkcgti0ONF9w/F12LwqW1GQjecEZZgohQmQlkDENRQOdWJINF4DaowPc6LM5tAd5/
kM666teylglDIgJnF2ThGEUrnkmavZvPsHuecWc/ZEYl+3NT7/gb46568UWPjXqbFo zQDzLozzqw+GABj+pXlC2fDBscesx++q5fBw5dPA=

Below is an example of a DNS TXT record for DKIM.

example._domainkey.itverx.com.ve.86400 IN TXT "v=DKIM1\; g=*\; k=rsa\; p=MIGfM
A0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqFGebZAOHfSGy9CWtA4Uads0zaXAy8TWtW9uIFbyIkFNC67fQVFVjsxlmcEg1oFNp2CrTYF1YNh2gB144
c+XY5GVM2fGEYAKx3iBxajWTzsx3SvpQtAZ2Bvf2mV+Te+JtlbpxVuiuiW2AIqwhk1ytTWspf/S3bM73XssV+/mh9wIDAQAB"

Phishing Protection

Domain-Based Message Authentication (DMARC)
Domain-based Message Authentication, Reporting and Conformance and builds on SPF and DKIM. DMARC contains instructions on what actions receiving gateways should take if a message fails the spoofing check. Like the others, it's configured as a TXT record in DNS.

_dmarc.example.net IN TXT "v=DMARC1;p=none;sp=quarantine;pct=100;
rua=mailto:dmarcreports@example.net"

That states the version as DMARC1, no policy (both SPF and DKIM are to be checked), the recommended action is to quarantine (or send to spam folders), that 100% of emails from example.net are to be subjected to the check, and reports should be sent to dmarcreports@example.net.

And, here's the thing: only 7% of companies using DMARC have it configured for "quarantine" or "reject." They use it for reporting purposes only, negating its value as an anti-spoofing mechanism. That's too bad because, in all three of these examples, they rely upon broad community/global adoption to realize any tangible benefit for those that deploy them.

Configuring SPF, DKIM, and DMARC doesn't prevent your receipt of spam and phishing, it prevents spammers and attackers from spoofing your email domain by sending spam and phishing to others. It's part of being a good citizen. Lack of immediate tangible benefit for the effort could be a big reason why adoption is low. Maybe default rejection of email from domains that don't use all three methods would be motivation to conform, but that's very unlikely to happen.

For added phishing protection, there are hardened email gateways and providers that have superb anti-spam capabilities



Avoiding Scams, Frauds, & Hoaxes

cipher
a PROSEGUR company

Train & Educate Your Staff

After completing your security policy audits, you can then enforce a written employee policy around data privacy and security. You will want to hold regular security trainings so that all employees are aware of these newly created policies – after all, people cannot voluntarily comply with unfamiliar policies. When establishing your security policy for employees, you might consider training on the following:

Control end-user access and privileges as it relates to the common policy called “least privilege.”
The use of various, unique passwords on computers or other devices used for work purposes.
Implement a documented system for departing employees, and vendors/contractors passwords, key cards, laptop access, etc.)
The importance of reporting suspicious data security leakage or data security breaches.
Create a policy that describes how employees should handle, dispose of, retrieve, and send data

Employees also need training on the types of modern phishing attacks. Phishing is the most common way for ransomware to spread within an organization. If you can train and educate your employees about the pitfalls and indicators to look for in a “phishy” looking email, your organization will be well served.

Cyber Tips

Make sure you make the staff training on security an initiative driven from the top down. If the staff sees your Leadership team committed to the training, the staff will also take it seriously.

Cyber Security Tips for Employees

Links in Emails: Clicking a malicious link in an email can lead to not just one compromised system but many. Before your employees click anything, they should know to check the link. They can do so by hovering over the link carefully to display the URL in the lower left-hand corner of the browser. All employees need to be extra careful of unsolicited emails with links containing malicious executable malware.

Spelling & Bad Grammar: Cybercriminals tend to not edit their scams for spelling, grammar, and other mistakes. Your employees should be trained to look for these inconsistencies whenever possible.

Active Threats : Your staff should also be aware of false threats such as account cancellation, penalties, or suspension. These threats instill fear within the employee but must be verified by a Supervisor before taking action.

Spoofed Websites: Cybercriminals are creating duplicates of popular websites with similar URLs only to lure employees into installing malware on their machine. Website spoofing is used to make people believe that they are interacting with a trusted, legitimate company or person. All employees should be trained to recognize inconsistencies and errors in URLs.

Helpful Resources

USA.gov Online Safety: https://www.usa.gov/online-safety
STOP.THINK.CONNECT Cybersecurity Resources : https://stopthinkconnect.org/resources
Federal Trade Commission Scam Alerts: https://www.consumer.ftc.gov/scam-alerts
Phishing.org: http://www.phishing.org/phishing-and-spoofing
Microsoft Safety and Security Center: How to recognize phishing email messages, links, or phone calls
http://www.microsoft.com/security/online-privacy/phishing¬symptoms.aspx

Planning for Security Incidents



cipher
a PROSEGUR company

Business Continuity Planning

Business Continuity Planning (BCP) is the creation of a strategy through which the recognition of threats and risks posed by unplanned events enable the company to continue business operations. Unplanned events include disruptions to electrical power or networks, attacks by a threat organization, natural disaster, civil unrest, and epidemic or pandemic events.

Along with a definition of roles and succession, communication plans, and descriptions of the business function and resiliency of various systems, a BCP contains collections of Disaster Recovery plans for each of those systems and defines Maximum Tolerable Downtime, Recovery Time Objectives, and Recovery Point Objectives. Professional security consultants will work with you to build a comprehensive plan, including procedures, processes, and testing, to ensure a state of continuity with business-critical systems.

A Business Continuity Plan will designate a Business Continuity Coordinator or Manager to execute the BCP if an unplanned event causes disruption. Not only does Business Continuity ensure operations continue, but it also means that it builds confidence with your customers and investors, and adds additional compliance benefits for various regulatory requirements.

Backing Up Your Data

Another commonly overlooked yet equally important aspect of your security strategy and business continuity includes backing up your data. In the event your data is compromised or deleted, you need to have a plan for its recovery. While 57% of IT managers have a backup solution in place, 75% of them were not able to restore all the data lost to ransomware.

Regularly planned backups ensure that your data isn't lost forever and is often used to restore your data if a successful attack takes place. A good rule of thumb is the 3-2-1 rule. You essentially keep three copies of your data on two different types of media with one copy stored in an off-site location. As an added measure of security, you can encrypt and password protect your backups that contain sensitive data.



Incident Response Planning

If your organization has just been breached or even had small security incident, an incident response plan will help you remediate quickly and effectively. A comprehensive incident response plan will require strategic planning and documentation but will benefit your organization during an incident.

Recent data shows us that data breaches are inevitable. It becomes increasingly important for companies to create an incident response plan.

An organization with an incident response plan will want to define the following to effectively manage a data breach when and if it happens:

- A response team that will be responsible for each area of the incident response plan (management, IT, information security, training, compliance and governance, and more)
- All communications methods for disseminating information about the data breach
- Who the organization should notify in the event of a data breach --- customers, partners, vendors, regulators, law enforcement, and any others
- Comprehensive logging and documentation throughout the data breach event
- All plans to contain and remediate the data breach

CIPHER Can Help!

CIPHER's Managed Security Services and Consulting Services can help your organization mitigate data breach risks using advanced monitoring and incident response techniques. Our global footprint, staffed by certified and expert security consultants and 24x7 Security Operations Center, helps financial institutions and many other global organizations with security detection, prevention, and response to complete their cyber security lifecycle strategy.

Founded in 2000, CIPHER is a global cyber security company that delivers a wide range of products and services. These services are supported by the best in class security intelligence lab: CIPHER Intelligence. Our offices a located in North America, Europe and Latin America with 24×7×365 Security Operations Centers and R&D laboratories, complemented by strategic partners around the globe. CIPHER is a highly accredited Managed Security Service Provider holding ISO 20000 and ISO 27001, SOC I and SOC II, PCI QSA and PCI ASV certifications. We have received many awards including Best MSSP from Frost & Sullivan for the past five years.

Our clients consist of Fortune 500 companies, world renowned enterprises and government agencies with countless success stories. CIPHER provides organizations with proprietary technologies and specialized services to defend against advanced threats, while managing risk and ensuring compliance through innovative solutions. Follow us at @ciphersec for more cyber security related content!

cipher
a PROSEGUR company