5 Easiest Steps

To Protect Your Company

From Cyber Attack or Data Loss

Sensible measures to reduce risk

Five Easiest Steps

What you can do to protect yourself without busting your budget. A list prepared from the perspective of a private business with limited resources.

Don't look here for technical, complex operations like deep vulnerability scanning, script-based penetration testing, code-based exploits, red teams and blue teams and so forth. These are all very useful activities and strategies, but they are beyond our scope here. Just know that such things are available. You can Google these terms and learn more if interested. There are many advanced strategies and tactics available, if you have the required resources (people and budget).

#1 Create a comprehensive but simplified Data Security Policy

There are many examples of data Security Policies available on the web. They vary according to the circumstances and characteristics of the organization. For example, public sector vs private sector, large vs small organization, type of data stored and used, and the industry or sate/country the organization operates in.

What should be included? Many samples can be found, with widely varying contents. Below is an outline, certainly very simplified, that can be used as a checklist for most organizations. Be aware that many of the items in this list tie in with the suggested contents for user awareness training described below.

1. Purpose
2. Usage
3. Objectives
4. Network Policies
5. Physical Policies
6. Mobile/Wireless Devices Policies
7. Acceptable Use
8. Security Incidents – Response

Somewhere, you need a bare-bones *Incident Response Plan* – this may or may not be part of the Data Security Policy. At the very least, list three people who need to be contacted if there is a data security incident, with their phone numbers and e-mail addresses. For each, list the information you plan to convey to them, and what decisions or actions they will need to consider. In other words, exactly what are you asking of them. For example, if one resource is the CEO, you may be asking her if the company should cease operations or alert law enforcement.

Print this out on paper and circulate it widely. Everyone who might be the first person to notice that something is amiss should know where the Data Security Policy is located and should understand its contents. Other policy areas may be addressed in separate documents or may be included in the overall Data Security Policy. Examples of additional policies may include a Physical Security Policy, a Network Security Policy, and a Mobile Devices Security Policy.

You have accomplished your first pass at this step when:
You have a complete Data Security Policy covering all the users, data, systems, and processors that your organization uses in its operations. Revisit your Data Security Policy when you have completed the remainder of the items in this list, and regularly thereafter.

#2. Make an inventory of your critical data, and how it is protected.

First, decide what data is critical – what data could you not operate without? What data, if it were lost or accessed by an unauthorized party, would cause major problems? For every file, list or data collection, identify exactly where it is stored, whether there are multiple copies, and how and when it is backed up.

It could just be a simple list of items like “Customer Master File, Main Database Server, Password and physical barriers” and perhaps “Secret Recipe for Coke, Boss’s laptop, login/password and SSL encryption”. This inventory is an important starting point, and a great exercise in finding out what you really know.

Suggested columns in your “Data Inventory” spreadsheet list:

1. Name of data store
2. Description and purpose
3. Confidential or critical for continued operation?
4. Where stored: (location, system, software)
5. Who has regular access
6. How it is protected
7. How/where it is backed up

The task of assembling the list may be more difficult than you expect. Be ready to ask questions of staff and managers – there may well be data stores that your IT team does not know about. When you have a complete list, you will have created something of value – be sure and update it regularly. Most people will store the list in Word or Excel and of course, print copies for dissemination.

If you have time, take it one step further. Create a "Device Inventory" - a separate inventory or all company-owned devices, including servers, routers, desktops, laptops, tablets and phones. Your list's columns might include item, vendor, operating system, who uses it, and an Asset ID if you have tagged all your devices (some organizations tag all assets, others don't). Compare your device list with your Data Inventory above Stores list – are they consistent?

You have accomplished your first pass at this step when:
You have a complete list of data stores, for both critical and non-critical data, with the location and other attributes as listed above. Consider a device inventory if time allows.

#3 Arrange user awareness training and knowledge tests

For online learning and testing, you can use an education platform like FlexTraining for easy course-building and management. But any flexible, authoring/delivery/tracking system will do. You may also determine that you will deliver these courses in-person. This option makes sense for a very small organization and/or one with all learners (staff) working in one location, with everyone available at the same time.

Tailor the material to your company or organization. But in general, your course should be organized into subjects and topics, and the subjects covered should include:

1. The Web and how it works

Topics: Why the web is not the internet, web server hardware, web server software, the cloud, dynamic vs static content, databases, HTTP, data encryption

2. Dangers of networks and the internet

Topics: Famous breaches, types of hackers, 24/7 connectivity, types of malware, phishing, social engineering, disgruntled employees, password hacking, tailgating, clickjacking, session hijacking, wireless scanning, ransomware, sophisticated exploits

3. Online security and privacy

Topics: Passwords, two-factor authentication, SSL/TLS encryption, best practices, the dark web, identity theft, web applications, designing for security, written policies

4. Protection: Anti-virus, firewalls

Topics: Malware protection, quarantine, continuous updates, vendors, network systems, configuring, bot scanners, IDS, IPS, host firewall, basic firewall, next-gen firewall

5. Laptops and mobile devices

Topics: Wireless world, hacking, defending, laptop considerations, mobile considerations, full device encryption, wireless encryption, WPA2, bluetooth, app security, mobile anti-virus, best practices

6. Troubleshooting & Recovery

Topics: Data recovery, logs, intrusion detection reports, incident response, recovery tools, user's role in recovery, lessons learned, modified procedures.

You have accomplished your first pass at this step when:
You have outlined, designed, authored, and delivered your first round of education to your staff and stakeholders

4. Establish Defense in Depth

“Defense in Depth” is actually very simple. It means you have in place more than one layer of protection for your information assets. For example, you may have a locked door to protect a server room, and then a password to actually log into the server itself. Or you may keep employee data in a database on a separate computer from your internet-facing web server, and also have the data with the database always be encrypted.

Look at the information inventory you created in Step #1 above. Are any critical data stores, such as customer lists or financial data, protected by only one barrier? What can you do about that?

You have accomplished your first pass at this step when:
For every information or system asset you have, you can identify at least two levels or components of protection for that asset.

5. Understand what else is available

The cybersecurity industry has grown along with the exploding threat landscape. There is now a tremendous variety of scanning, analysis, logging, selection and prevention tools. Services and training are also available from many companies. Below are just a few technical tools that can be used to strengthen your data defenses and locate vulnerabilities.

Zenmap – Network, software, version and port scanning. Find the various components and what kinds of software and services are running on them. Zenmap is a free tool with amazing power and versatility. It is the GUI version of “nmap” and can scan any local or remote device with a network connection.

SIEM software – Pulls together various technical, security, and activity logs to present a comprehensive picture of what is happening on your network. Missing details, activity or data may mean that something has been tampered with or maliciously deleted.

Nessus – detailed vulnerability scanning. A vulnerability is essential a weakness or a potential path that an attacker can exploit to harm your operations or steal your data. Nessus is a complex tool that uses scripts and options to simulate attacks on just about any kind of device or server.

There are also free tools available for the specific purpose of scanning web applications and looking for vulnerabilities related to forms, data, web browsers, etc.

Consult your cybersecurity professional for additional tools and options.

You have accomplished your first pass at this step when:
You have identified several additional technologies and procedures that are available, given additional time and money, to further enhance data security.

Five Questions and Answers

1. I see the huge data breaches in the news. So these cyberattacks only happen to big companies, right?

No - many attacks and data breaches happen to small companies, organizations, and government departments. A recent large cybersecurity conference featured a full-day workshop for small governments and non-profits. It can happen to anyone.

2. There are so many bad actors out there and such a wide and growing variety of threats. Has it gotten to the point where there is really nothing that can be done to avoid a successful attack?

Well, there is a LOT that you can do to keep your business and your data - and your customer's data - safe. No one is 100% protected, but there are definitely *best practices that can be followed which greatly reduce the likelihood of a serious security incident. In fact, many steps that you can take are very economical, and are sometimes referred to as the “low hanging fruit”. And for those with additional resources, there are many technical, procedural, and user-focused measures you can apply to create additional layers of protection.*

3. Will developing defensive policies and testing our security disrupt our daily operations?

It should not be allowed to disrupt normal business functions. Yes, if you authorize active - rather than passive - probing, testing and scanning on live data, during business hours, using improper tools, there may be disruption. To avoid this, we make smart choices and utilize safe practices to avoid damage, disruption, and confusion. And we also agree on a detailed plan ahead of time.

4. But this is really just an IT problem, right? Aren't they paid to protect our data and systems?

Information Technology teams are certainly involved in protecting assets like computers and sensitive data. However, good data security is everyone's responsibility, from top management down to every employee or contractor. Targeted user education, best practices, and common-sense planning can help create a "culture of security" that is the foundation for good data protection. It all starts with a customized, comprehensive Data Security Policy document.

5. After we engage in a one-time cybersecurity project, then can we get back to business-as-usual?

Almost all modern companies, departments, and organizations rely on connected technology to help them perform their mission. And with the growing threat landscape that changes every year, maintaining vigilance and revising plans and policies are an ongoing priority. There will never be a day when we can stop paying attention to the cybersecurity responsibility which we all carry. There may be additional effort and resources deployed to create initial plans and guidelines, but recurring training, planning, and vulnerability testing are here to stay.