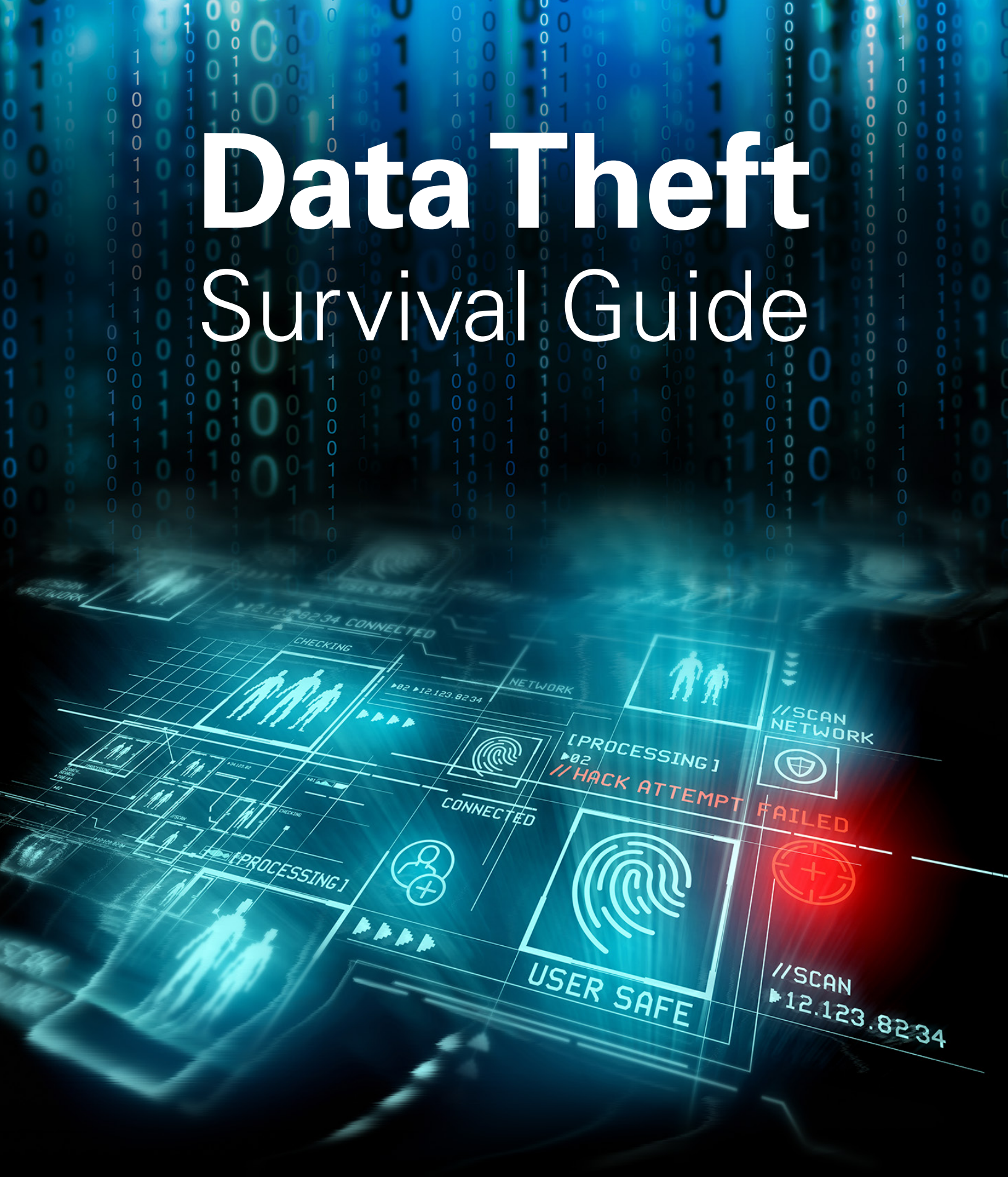
Data Theft
Survival Guide



Zettaset

Data breaches and the loss of sensitive business information are the biggest threat that organizations face today. While lone wolf attackers are still out there causing their own brand of mayhem, cyber crime syndicates comprised of hacking professionals are the real concern[1]. All industries and organizations, regardless of their size, are at risk because of the valuable personally identifiable information (PII) of customers and employees that their databases hold. Compounding this problem, with Internet of Things (IoT) devices becoming ingrained in our business operations, we are exposing ourselves to new risks.

There is money to be made in hacking through selling information on the black market or holding valuable information for ransom. Cyberattackers and their modes of attack are evolving to exploit new technologies and take advantage of security gaps.

Unsurprisingly, it can be difficult to navigate these rough cybersecurity waters and completely avoid a data breach. If you are the unlucky victim of a massive data breach, there are many questions for you to answer – and a ton that needs to get done. That's why Zettaset has put together a Data Theft Survival Guide to help you escape unscathed if the unthinkable does occur.

So, how can you set yourself up for success and minimize the likelihood of a data breach? We'll examine that here and provide guidance on how to respond in the event your organization is affected by a breach.

Before a Data Breach Hits

It's time to act quickly. Seal the gaps in your data security. Examine your overall cybersecurity plan. There is no good time for a data breach to hit, and it can strike without warning. You've got little time to spare, but by following these steps, you can help prevent a data breach and better protect your data if you are affected.

Step 1: Everyone Needs to Join "Team Cybersecurity"

Before you embark on this journey to secure your organization, it's important you have the right mindset. Take security seriously! What we mean by this is you need to create a workplace culture that values customer and employee privacy. The best way to protect your organization's information is for everyone to join "Team Cybersecurity."

Encourage all employees to speak up if they recognize something that could be perceived as a security threat. This can be something small, like printing a customer's credit card information for an invoice to a public printer. Or, it can be something more threatening like noticing a suspicious email or an unusual alert to update a specific software application.

Your cybersecurity team should have a way to share these internal concerns and observations, and address them in a timely manner. Introducing an incentive program for employees who detect significant vulnerabilities can increase involvement in the program.

[1] https://www.csoonline.com/article/3215111/security/security-it-s-9-biggest-security-threats.html

Continued employee education can help participants better understand the difference between real data security threats and minor issues, and help reduce the number of "false positives".

Now that you've recruited your entire company in the fight against data theft, it's time to focus on important cybersecurity measures.

Step 2: Perform Timely Updates

The catastrophic Equifax data breach can be traced to the failure of the company to download a patch[2]. This is precisely why timely updates are no joke when it comes to data protection.

When your software prompts you that a new update is available, make sure you perform the update. Despite being such an obvious step in preventing data breaches, users still forego updates regularly. Why? There are a few reasons.

Incompatibility

Software is always in flux. It's a work in progress, and developers are constantly making revisions and upgrades. Unfortunately, that means that software that is compatible one day might not be by the time the new update is out. Incompatibility is a huge reason why software updates aren't deployed in a timely matter.

There is often fear that performing an update may conflict with another element in your IT stack. Meanwhile, there are many times when the IT team knows for certain that making an update in one place will mean something else won't work. Teams need to find a fix, and perhaps switch to an alternative tool. Inconvenient as this may be, it beats having to deal with a data breach.

Understand what software you are using and which issues might occur if an update causes an incompatibility. Have a backup plan in place, and work to eliminate tools that might cause an unresolvable conflict within your IT stack.

The Wrong Person Gets the Notification

Don't let this happen to you! Email notifications might be erroneously going to a former employee, an outside contractor, or someone on your team who does not realize he or she is responsible for this update. Make sure you have a system in place and that the notifications for patches and updates go to the right person. When someone on the IT team leaves the organization or transfers to another department, immediately update your notification settings.

Consider sending important software update notifications to multiple users. Create a tiered structure so everyone understands who is the main contact responsible for the update and who, in turn, is the back-up. This way, you don't find yourself in a situation where everyone thinks someone else performed the update...but didn't.

[2] http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Users Assume Automatic Updates are Enabled

We work so hard to automate everything in our lives that sometimes we just assume things are automated when they are not. This occurs in our personal lives with automatic bill pay, and it also occurs in our professional lives with software updates.

Despite being notified (and being the right person), and knowing that this update will not create an incompatibility with your other software, you may ignore the update simply because you think it's already been applied. Never assume that updates will be automatically applied for any software application.

A setting may have changed since the last update that turns off the automated feature. Or, a new update may require administrator approval that the automatic setting cannot bypass. Whatever the reason may be, double-checking is never a bad thing when your organization's sensitive data is on the line.

Step 3: Get Data Encryption

Uber[3], Equifax[4], and Yahoo[5] all failed to deploy vital encryption technologies that would have protected their stolen data from being usable as soon as it was taken by hackers. These organizations also incurred significant penalties for not properly protecting their customers' data. And of course, the public perception of these businesses was immeasurably tarnished.

Encryption is the act of encoding data to make it indecipherable to anyone except the person or persons who possess the encryption key. While encryption doesn't prevent data attacks and breaches, it makes any stolen data unusable to hackers because it renders the data unreadable.

Additionally, some forms of data encryption prevent the act of data manipulation. This is a rarer, more malicious type of data breach where the goal is to change the data as opposed to steal it. This is usually carried out by groups looking to damage a specific company or individual for some sort of political or personal gain, as opposed to financial gain.

The decision to not encrypt your data is a risky one, as peripheral security tools such as firewalls and intrusion protection systems are continually being bypassed by hackers, and do not protect the data itself.

Step 4: Back Up Your Data

In the event of a data breach, it's important to make sure you do not place all of your eggs in one basket (or all of your data on one server). This is also incredibly important if your server simply fails and/or your data is corrupted.

Backing up your data allows you to reconcile unauthorized changes in the event you are breached and data is modified. It also puts you in a better position if your data is held for ransom. Make

[3] http://fortune.com/2017/11/22/uber-data-breach-lawsuit/
[4] https://www.cbsnews.com/news/equifax-ex-ceo-hacked-data-wasnt-encrypted/
[5] http://www.tomshardware.com/news/e2ee-yahoo-mail-hack-spying,32857.html

sure all of your data is encrypted and that the keys are kept strictly separated from the data store and in possession of trusted individuals.

Keep your data stored in different (but easily retrievable) formats. Some security professionals recommend making two copies of your data. For enterprise organizations, this should be standard practice.

Step 5: Vulnerability Assessment and Penetration Testing

Cybersecurity is not an event, it's an ongoing process. While you may upgrade software and patches when prompted, changes to code might create unforeseen vulnerabilities. Hackers are constantly probing systems for any susceptible weakness. You don't want a hacker to find out about a security weakness before you do.

Performing vulnerability assessments and penetration testing in tandem allow cybersecurity teams to identify possible outsider points of entry.

A vulnerability assessment is the process of scanning your system for any weak points. Penetration testing is the act of asking someone to infiltrate your system and take what they can. This might sound counterintuitive, but performing a test like this either internally or with an outside, verified team, identifies the strength (or weakness) of your cybersecurity approach.

After the Data Breach

Uh oh. You couldn't make it through without getting breached. Your data has been stolen, held for ransom, or manipulated in a way to make it unusable. Now what?

Step 1: Contain the Threat

Now that you've identified an intruder in your system, you need to kick them out and stop them from getting in again. There may be multiple hackers within your system, so be careful to track them accordingly.

Your entire security team needs to be available to assist with this. Identify and secure the main access point (and any additional access point the intruder may have created after gaining initial access).

Step 2: Identify the Vulnerability

So, how did it happen? Was it a missed patch update? Was it a lack of data encryption? Or, was it a new type of cyberattack your organization (and any other organization in a similar position) wasn't prepared for? Knowing the source of the threat will show you what you need to focus on in the future.

Unfortunately, someone will have to take the blame. It's not often that data breaches occur without finding someone at fault. Knowing the nature of the vulnerability, who (or which team)

was responsible for it, and why it was missed gives you insight into the efficiency of your process. It will also likely result in the termination of at least one employee.

This won't just help your team improve, it will enlighten other organizations on what precautions should be taken in the future. Since the nature of cyberattacks is constantly evolving, and the ways in which hackers gain access is never quite the same, this is vital information that should be shared. It is also important that you give your customers and other stakeholders peace of mind by identifying the issue and confirming that you've secured it.

Step 3: Determine What Was Stolen (And How Much)

The intent behind every data breach is different. Not everyone is after Social Security numbers and email addresses. Some hackers may be interested in banking information, electronic health records (EHRs), or in manipulating data for political or economic gain.

After falling prey to a data breach, it's important to inventory everything that was stolen or changed. This is essential when you are disclosing the nature of the breach to the media, as well as understanding the attacker's motives. Knowing what was stolen gives you an idea of what is likely to happen to the data and what precautions victims should take. Understanding what information from your business is valuable to hackers will also allow you to better safeguard that particular information in the future.

In cases of manipulation (tampering) of encrypted data, identifying the data that was hacked is of the utmost importance. This is not just so organizations can understand the motives of the hacker, but so they can correct their now-corrupted data.

Data manipulation refers to modifying the data in such a way to render it unusable. If you were prepared for a data breach, you'll have backup data servers in place. Organizations can recover this information using their backup devices and actually determine how hackers changed the data. Data modification can be used for nefarious activities. Take for instance bloodwork tampering with the intent to harm a specific individual, or making unauthorized changes to a no-fly list. Being able to detect unauthorized modifications to encrypted data is essential since the potential danger to personal and public safety is extremely high.

Step 4: Announce the Breach Immediately

Don't suffer a total PR disaster like countless data breach victims before you. Tell the public, tell your customers, and tell your vendors. Whoever is at risk needs to be notified immediately. This isn't just to cover yourself, it's actually the law.

Forty-eight U.S. states, Puerto Rico, the District of Columbia, Guam, and the Virgin Islands all have legislation requiring that individuals be notified if PII has been put in jeopardy because of a data breach[6]. The GDPR gives European companies, and companies that deal with European customers, only 72 hours to report a breach as soon as it happens[7].

[6] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[7] https://gdpr-info.eu/art-33-gdpr/

Do not delay announcing that you've been breached, as it will eventually result in negative repercussions for your brand and customer loyalty. When it comes to announcing to the world that you've been hacked, you're better off doing it sooner rather than later.

Step 5: Offer Your Consumers Recourse

It's standard procedure for organizations to offer customers one to two years of credit monitoring services if their data has been compromised. In 2017, the state of Delaware introduced new legislation that stated a breach of 500 or more individuals requires that the affected organization purchase credit monitoring services for their affected customers[8].

Don't allow government legislation define how much you offer your customers and employees affected by a data breach. Go big when providing your customers with recourse. History tells us that data breaches can lead to major distrust of the affected brand[9]. After Target's 2013 data breach, their sales fell 46 percent the following quarter. Providing immediate support for your customers (and admitting that you have an obligation to make this right) can mitigate a fall in sales and loss of trust.

Step 6: Make Sure it Doesn't Happen Again

In these times, one data breach is hardly forgivable. Suffering multiple data breaches in a short span is a recipe for chapter 11. According to a report released in October 2017, 66 percent of small businesses would either go out of business or shut down for at least one day if they suffered a data breach[10]. In another report, 76 percent of those interviewed said they would stop using a company that suffered more than one data breach[11]. For this reason, it's important that you do everything in your power to prevent a data breach from happening again. After all, you are now a target. You have sent a message to the hacker community that you are lax on security. It's time to recreate your image as a company that takes data security very, very seriously.

Those responsible for the vulnerability will either need to be disciplined or dismissed. Whatever led to the vulnerability will require you to examine your business processes and modify your security operations procedures. It's also vital that you re-examine all of your security processes.

Is your threat detection software doing its job? Is your data encryption sophisticated enough for your organization's needs? Do you have a security-first mentality within your organization? Address all of these questions and respond accordingly.

Encryption is a vital piece of the surviving-a-data-breach puzzle. Get a demo of Zettaset XCrypt™ today.

---

[8] https://www.insideprivacy.com/data-security/data-breaches/delaware-amends-data-breach-notification-law-to-require-credit-monitoring-attorney-general-notification/

[9] http://customerthink.com/what-consumers-think-about-businesses-post-data-breach/

[10] https://www.techrepublic.com/article/66-of-smbs-would-shut-down-or-close-if-they-experienced-a-data-breach/

[11] https://www.darkreading.com/vulnerabilities---threats/survey-customers-lose-trust-in-brands-after-a-data-breach/d/d-id/1325570?

Zettaset

465 Fairchild Drive, Suite 234, Mountain View, CA 94043

www.zettaset.com // +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.