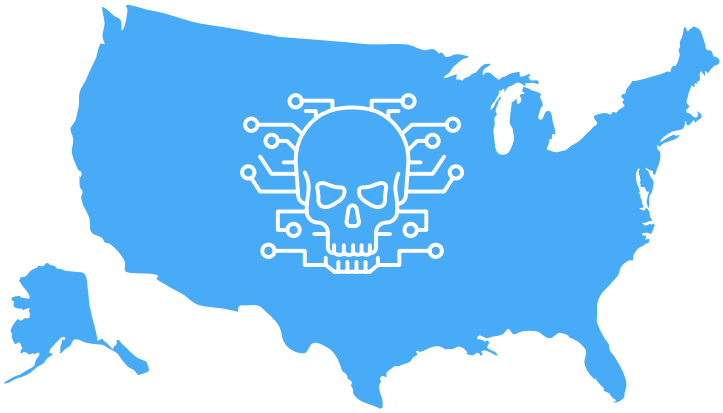
Section I

The Cybersecurity Crisis

Cybersecurity is a massive concern for every modern business. According to data from the Identity Theft Resource Center (ITRC), in 2017 alone, there were approximately 680 *confirmed* data breaches among U.S. businesses—breaches that compromised 159,365,480 records. To put that into perspective, the total population of the United States is, according to the U.S. and World Population Clock, 326,971,209 as of January 1, 2017.

This means that the personal data of roughly *half* of the country's population were stolen from businesses in 2017. Another 2,910,117 records were compromised from attacks on the banking industry.

The most sobering thought is that these are just the statistics for data breaches that were *confirmed* by the ITRC—it cannot account for all of the breaches that went undetected or unreported.



> ***...in 2017 alone, there were approximately 680 confirmed data breaches among U.S. businesses—breaches that compromised 159,365,480 records.***

The Cybersecurity Crisis

Safeguarding Your Sensitive Data

The unfortunate truth is that you cannot stop 100% of all breaches. There are simply too many threats out there (and too many unknown exploits) to ever guarantee absolute protection from everything.

From the pre-existing exploits of programming errors in your IT assets, to internal attacks by employees abusing their access privileges, to simple mistakes by employees who accidentally transmit something they shouldn't, there are numerous ways for malicious actors to breach your cybersecurity measures. A dedicated attacker or group of attackers can eventually breach almost any defense.

However, that doesn't mean that you have to make things easy for attackers. While you might not stop absolutely every attack, you can limit your organization's exposure to risk and prevent the majority of attempts by following a few basic elements of cybersecurity and maintaining good "cybersecurity posture." By cybersecurity posture, we mean the overall strength of an organization's cybersecurity measures. A company with a strong cybersecurity posture is one that has all of the necessary elements in place to prevent or at least limit the impact of attacks on the organization.

The eight most basic elements of a strong cybersecurity posture are:

- Asset Management
- Risk Management
- Access Management
- Security Controls
- Incident Management
- Threat Management
- Security Education, Training, and
- Disaster Recovery & Business

These eight elements form the basis of a strong cybersecurity posture—but what comprises these elements? More importantly, how can you make sure you're addressing each of them in a way that maximizes your protection from security breaches?

Section II

Anatomy of a Strong Cybersecurity Posture

> **A strong cybersecurity posture is one that minimizes your exposure to risk. It also means having a strong grasp of the basic elements of network and data security. Compuquip's research into data breaches shows that many attackers start their intrusion attempts by exploiting gaps in cybersecurity basics—so you should make sure that you've covered them.**

Additionally, it is important to get management at all levels of the company to not only "consent" to upgrading your company's cybersecurity posture, but to embrace the changes. Getting management to "buy in" to the need for cybersecurity is an important first step. When upper management supports your cybersecurity program and models the behaviors needed to sustain it, you're more likely to get everyone else to take cybersecurity seriously.

The following sections will list the basic elements of cybersecurity and what each entails so you can identify opportunities for improving your security posture and make a case for cybersecurity to your management team.