GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Spencer, Jimmy

"Why is Cyber Security Important in 2019?"

securityfirstcorp.com

Security First Corp.

06 May 2019

The URL: https://securityfirstcorp.com/why-is-cyber-security-important/

Accessed: 15 October 2019

Synopsis: Why is cyber security important all of a sudden? Not that long ago, it was primarily something for only the techies to worry about. Corporate leaders widely viewed it as the responsibility of their IT department. Many thought – perhaps naively, it now seems – that so long as the right firewalls, antivirus packages and encryption tools were in place, they could leave IT security to the experts and focus on the other myriad elements of running a business.

Why is Cyber Security Important in 2019? - SecurityFirstCorp.com

Jimmy Spencer, Senior Security Architect

Why is cyber security important all of a sudden? Not that long ago, it was primarily something for only the techies to worry about. Corporate leaders widely viewed it as the responsibility of their IT department. Many thought – perhaps naively, it now seems – that so long as the right firewalls, antivirus packages and encryption tools were in place, they could leave IT security to the experts and focus on the other myriad elements of running a business.

Presumably, you're now very much aware that cyber security is something nobody can afford to ignore. Unless you hide from the world's media, you must know that hacks and data breaches regularly affect firms of all sizes. Often these incidents are significant enough to make the front pages, causing irreparable reputational damage to the companies involved.

If you're not worried about cyber security, you should be.

So what's changed?

Fundamentally, we're living in a far more technologically-advanced world than we were as recently as a decade ago. If you need convincing of this, consider the fact that the iPad has only been around since 2010, and the iPhone only came out a few years before that. Average broadband speeds have increased by roughly five-fold in the last decade, making it possible for businesses and individuals to do far more online.

A particularly valid example of the change that this has facilitated is the rise in cloud services. Nowadays, most businesses take for granted such things as easy online document sharing, email that's available on every device, and databases accessible from everywhere. While the years have seen enterprises increasing deployment of business-critical applications in the cloud, Amazon's Elastic Compute Cloud has only been available since 2006.

The rise of cybercrime

This rise in the widespread use of technology brought with it a rise in cybercrime. For hackers, the possibilities increased exponentially, along with the potential rewards. At one end of the scale, you have "script kiddies" hoping for a modest payday from unleashing some ransomware on a single computer. At the other, there are "state-

sponsored" hackers, who've switched to cybercrime as a method of war, viewing it as "cheaper, faster and easier than traditional conflict."

The fact that cybercrime now permeates every facet of society shows why cyber security is crucially important.

Damage to companies

There have been so many hacks and data breaches in recent years that it's easy to produce a laundry list of household name brands and organizations that have been affected.

Just a few examples are:

- **Facebook**, the social media giant had over 540 million user records exposed on Amazon's cloud computing service.
- **First American Corporation**, had 885 million records exposed in a data breach that included bank account info, social security numbers, wire transactions, and mortgage paperwork.
- **Equifax,** the global credit ratings agency who experienced a data breach that affected a staggering 147 Million customers. The costs of recovering from the hack were recently estimated at $439 Million.
- **The UK National Health Service (NHS),** which was temporarily brought to its knees with a relatively rudimentary ransomware attack, resulting in cancelled operations and considerable clean-up costs. This specific attack became particularly embarrassing for the UK government, when it emerged that "basic IT security" could have prevented it.
- **Yahoo,** the web giant that suffered a breach affecting every one of its three Billion customer accounts. Direct costs of the hack ran to around $350 Million, and while it's harder to quantify reputational damage, it's probably fair to say that Yahoo is not the first port of call for consumers seeking a safe and secure place to host an email account!

While these are just a few examples of the many headline-grabbing hacks of recent years, it's important to remember that there are plenty more that don't make the front page but still harm or destroy companies of all sizes. While *Wired* reports on cybercrime incidents at smaller companies such as MyHeritage, a DNA testing firm, Typeform, a survey company, and the UK's University of Greenwich, there are thousands of other hacks that don't even make the news.

In fact, one particularly chilling statistic is that there are now over 4000 hacks every single day using *ransomware alone*. It's extremely misguided for anyone to think their company couldn't be affected.

Endless statistics

It's incredibly easy to find cybercrime statistics to shock and surprise people and prove strong reasons for cyber security. In fact, it's fair to wonder if people may have become a little desensitized to them, or that the sheer scale of the numbers makes them hard to take in.

For starters, it's estimated that the global cost of cybercrime for 2017 added up to around $600 Billion. The number mounts up every year, and by 2021 pundits are suggesting a figure of $6 Trillion per year.

But perhaps it's better to focus on statistics that are more relatable to you personally – in your role in your business, for example:

How about the fact that 54% of firms had their network or data compromised last year? If you're one of the few people yet to experience being in the thick of such an attack, the fact that it happens to more than half of companies in a year suggests it could well be your turn soon.

Or, perhaps you could keep yourself awake by considering the average cost of recovering from a cyber attack, which is estimated at $5 Million. If you run a smaller business, this might seem like an enormous figure, but these things are proportional. Plenty of small businesses could be wiped out by a bill of $50,000. This is reflected in a final statistic that's widely quoted: 60% of small businesses who experience a major cybercrime incident go out of business shortly after.

Standing up to the threat

So, with all this in mind, "why is cyber security important?" should now be a question with a clear answer. So, what can you do fight against the growing threat? Here are some suggestions:

1. Keep informed

It's no longer realistic or fair to expect an IT department to mitigate every IT security risk (and in reality it never really was). Many modern cyber security threats originate from social engineering, user error, exploits to web browsers, and other things that technical teams can only do so much to protect you from.

Cyber security is something everyone needs to take notice of, and a huge number of incidents are caused by people ignoring mainstream advice around avoiding clicking on suspicious links and maintaining secure passwords. Hackers love "low hanging fruit," so don't allow you or your teams to be that fruit!

2. Move beyond antivirus

Antivirus software is still an essential part of the IT security armoury, but it's not enough – by itself – to protect from modern threats. Technical teams need many more tools, resources and solutions, and some of them are expensive. However, they're not likely to be as expensive as the cost of clearing up after a cyber attack.

3. Get insured

The market for cyber security insurance has boomed in the last couple of years, and it's now something that companies of all sizes need to think about. Cyber security insurance isn't only about protecting against financial risk. If your company is hit by a data breach, there's a lot of damage to contain, and you may need help with that from the kind of experts and damage-limitation specialists your insurer could provide.

4. Take your flow of data seriously

Another good example of why cyber security isn't merely a technology issue is how easy it is for a member of staff in any department to cause a data breach. A breach is still a breach whether it's caused by a hacker in a darkened room attacking a network, or a distracted employee leaving an unencrypted personal device on public transport.

Recent legislation, such as Europe's GDPR (General Data Protection Regulation), has forced many companies to take a really good look at the importance of cyber security, and how they store and process data. Instead of feeling ground down by this weight of this compliance, another option is to use it as an opportunity to really think about your company's use of data. With some simple thought, it's relatively easy to eliminate weak spots in processes that could expose data, cause a breach, or simply make life easier for hackers than it needs to be.

5. Think about backup and recovery

A company is hit by ransomware every 40 seconds, but the irony is that no firm needs to pay a ransom if their backups and disaster recovery efforts are on point. Yes, such a cyber attack will cause annoyance and disruption, but if a backup is there, there's no need to pay hackers any money.

This probably strikes you as an extremely basic point. However, it's clear that plenty of companies drop the ball. Otherwise, there wouldn't be a statistic saying that nearly half of affected US companies end up *paying* ransoms to hackers! This indicates that an awful lot of companies don't manage to get business continuity right, however obvious the need for it may seem. This is not only about ransomware – reliable backups back all kinds of hacks and breaches easier to recover from.

Why is cyber security important? Hopefully, the answer is now clear! It's not going to get any less important in the coming years. Numerous studies point to a predicted increase in attacks, and it seems likely the statistics will get more shocking and the financial losses more breathtaking. While we continue to hand over more elements of modern life to technology, this shouldn't surprise us.

Contact SecurityFirstCorp.com for help and advice on your company's cyber security.