

Serious security
professionals
protect their
people and
their data.

ebook




Cybersecurity Made Easy

Why & How to Secure Your Data



OSTENDIO



Every second of
every day we create
new data

Over 300 data breaches have involved the theft of 100,000 or more records each.

By the year 2020, approximately 1.7 megabytes of new information will be created every second for every human on the planet.¹

As the pace of data generation increases, so does our reliance on it, both in business and in our personal lives. With the world's volume of data growing exponentially, there's a greater avenue of opportunity for cybercriminals to exploit. Over the past 10 years alone, over 300 data breaches have involved the theft of 100,000 or more records each – and these are just the ones publicly disclosed. Whether your business is large or small, financial, healthcare, technology, municipality or manufacturer – you're at risk. And only serious security people are willing to take the steps necessary to protect their people and their business so everyone's data is safe.

How did we get here? What does your cybersecurity program's strength or weakness mean to your business's stability and reputation? How do you preserve day-to-day operations with the looming, very real danger of cyberattack? Do you focus on data breach prevention or response?

The answers are multi-fold and often confusingly complex. Let's simplify.

**Data breach impact
statistics:²**

EQUIFAX

143 million+ Americans
likely affected

**Q3 2017 TO-
DATE**

2 million+ health data
records

2016

15.4 million U.S. identify
fraud victims



Data Makes a Business Attractive – Not its Size



The Chinese have penetrated every major corporation of any consequence in the United States and taken information. We've never, ever not found Chinese malware.

MIKE MCCONNELL

ex-NSA Director

Cybercrime is a profitable venture. It's an ugly reality that stealing data such as personal information, or financial history gained from credit card accounts, the trade secrets of corporations and intellectual property – is how cyberattackers make a living.

When it's not about financial gain, the threat to data security may come from a malicious insider or a hacktivist. Consider all of the following when you develop your privacy and security strategy.

- 1. Internal Threats:** Disgruntled employees or the human error of someone clicking a malicious link in a phishing email accounts for nearly 50% of data breaches. Third-party vendors are another significant internal risk. Gaps in security equal a back door into your system, e.g. Target's client record breach.
- 2. Hacktivist:** In broad terms, hacktivism is the use of technology to signal dissent, often with a political agenda. Anonymous is probably the most notorious group. Recently, we have seen hacktivist groups declare war on groups like ISIS, trying to bring down their social networking.
- 3. Cybercriminal:** The increasingly sophisticated cybercriminal may be a lone wolf or organized corporation. Ransomware-as-a-Service is one lucrative trend surfacing a lot in 2017. Cybercriminals don't care about breach size – they care about exploiting vulnerabilities. Although the cost of a data record has decreased from \$158 to \$141 per compromised record, the sheer amount of data available means that cybercriminals will continue to profit.
- 4. Corporations:** Corporate espionage is nothing new, it's just now being done digitally.
- 5. Governments:** Our increasingly global economy digitally connects us more than ever. That's a concern when geopolitical turmoil affects trying to protect data. Foreign nation-state attributable incidents have grown 140% over the past three years. The Petya ransomware attack in June 2017 impacted businesses, government agencies and critical infrastructure, and is widely suspected to be a state-sponsored attack against the Ukraine rather than a vicious for-profit cyberattack.



Know your Data. Know Everything About It.

Know what you know. Own – and fix – what you don't. There's too much attention on cybersecurity for playing the victim to hold water with shareholders, consumers or regulatory agencies.

Top 5 Must-Knows about the Data You Protect⁸

1

KNOW THE DATA YOU HAVE

When you classify data by sensitivity, you can focus on protecting the most valuable.

2

KNOW EVERYWHERE YOUR DATA LIVES

Copies may be both in storage and in transit at any time.

3

KNOW WHO HAS ACCESS TO YOUR DATA

Whether theoretical or incidental access, understand who has access and what level of access they have.

4

KNOW WHAT THEY'RE ALLOWED TO DO WITH THE DATA

Access to data must come with rules of use to ensure the data isn't shared or exposed in an unauthorized way.

5

KNOW HOW THE DATA IS PROTECTED FROM UNAUTHORIZED ACCESS

Level of encryption, physical security, access management, and identity protection are all valuable tools, but if they only protect one version of the data, then they become ineffective.

Avoid the temptation of starting at #5. Once you understand what data you should be protecting, then select hosting providers, encryption methodologies, and the needed level of cybersecurity tools. You can spend tens of thousands of dollars on sophisticated cybersecurity tools but neglect the most critical part: people.

Ostendio's Ostendio can show you where your data lives, who has access to it, and when it's being accessed. Ostendio can help you build, manage and maintain your cybersecurity and information management program quickly and efficiently.




Make Cybersecurity Everyone's Business

Ransomware dominates the headlines yet the most likely source of breach occurrence remains human error. Turn the tables by building a culture of cybersecurity within your organization – and your employees become your front line of defense.

How to build a culture of cybersecurity⁹

- Look at security from the bottom, up. Everyone needs to know exactly what their role is when handling sensitive data. From an entry-level employee to the C-suite, anyone can create data vulnerability. Which leads to...
- Invest in frequent training. Employee awareness training no matter your title or function is essential to fill the gaps that information security tools alone can't close.
- Keep education simple. IT is full of acronyms and jargon; use layman's terms to explain ideas and train. Create realistic scenarios for everyday business tasks. Realize that digital adults – people who grew up with iPhones in-hand – share everything online, with a different attitude toward what should or shouldn't be private.
- Focus on security basics. Turn auto-updates on, set password requirements, and shut down computers on a regular basis to allow for security patches, back-up data frequently, store off-site for protection and a quick restore.
- Get senior leadership buy-in. If management hasn't embraced and evangelized the importance of cultural cybersecurity, no one else will. The IT department may carry the flag, but it's senior leadership's job to plant it and rally everyone around it.



When cybersecurity fails, be ready to respond.

Less than 50% of companies feel confidence in their data breach response plan – or in their ability to roll it out.

A data breach is an equal opportunity occurrence; it can happen to any company. But preparedness pays off. With a solid security incident response plan that includes scenario-driven data breach responses, your team will know what actions they need to take.

When a breach occurs, you won't have time to plan, you need to be able to simply hit "Go" and roll out your response plan. The first action item? Know who to call and when. When there's a set process to follow, not just a checklist, everyone knows what their responsibility is and can execute right away.

As an example, here are 4 action items for immediate security response in case of ransomware:

1. As soon as you realize there's an issue, disconnect.
 - If you're on a network, immediately notify your IT department.
 - If you received an email from someone externally that sets off ransomware, notify them, too. It may have been a fake email or they may not know they're infected.
2. Hit "Go" on your Security Incident Response plan. Communicate quickly and effectively with stakeholders and users.
3. Go to backups that weren't connected to the infected network. It could significantly limit damage and downtime.
4. Notify your FBI field office right away or file a cybercrime complaint. Make no mistake, ransomware is criminal.



Cybersecurity is King. Isn't it?

Creating a culture of cybersecurity is a large part of a deeply needed change in how we approach sensitive data protection.

Data breach prevention works. Investment in a robust cybersecurity program works. Security awareness training works.

Humans hold the answer to – and are the root of – the cybersecurity challenge.

It holds true that no matter your industry, the leading cause for cybersecurity breach remains in the human capacity for error. We use public Wi-Fi at the airport to view account balances and send money, check in on social media to share our lives with anyone who's watching and track our personal health information in an online record system. Overwhelmingly, the convenience factor overrides the risk factor.

We're transparent in nearly everything except proving that we're doing everything possible to protect sensitive data.

Our global business-to-business interconnectivity calls for transparency as never before. You need to know that if you're doing everything to protect data – and ongoing business operations – so is your business partner.

Contact Ostendio to learn more about how Ostendio can help simplify your cybersecurity and compliance needs.

We're in an ongoing battle to protect sensitive data.

Your best defense:

Combine human readiness with advances in technology. Intertwine prevention and response: perimeter security, firewall and threat detection, plus cybersecurity awareness throughout the masses who use it.



About Ostendio

Ostendio's Ostendio™ helps companies to build, manage and demonstrate their information security framework. The Ostendio platform provides an enterprise view of an organization's cybersecurity program. Ostendio's unique bottom-up security approach provides a workflow solution which engages every employee and manages all aspects of security and compliance which allows organizations to easily report their security posture to internal and external stake-holders. With Ostendio, customers can ensure they are secure and compliant.

Ostendio is headquartered in Arlington, VA and has customers in North America, Europe, the Middle East and Australia. For more information about Ostendio's Ostendio, please visit www.ostendio.com.

Everyone Secure

Welcome to the next generation of security.

Ostendio is the only risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

[Schedule a demo today.](#)

References:

1. <https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#413e9c3b17b1>
2. <https://www.usatoday.com/story/money/2017/09/17/equifax-data-breach-number-victims-may-never-known/670618001/>
3. <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>
4. <https://www.ibm.com/security/data-breach/>
5. <http://money.cnn.com/2015/03/13/technology/security/chinese-hack-us/index.html>
6. <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/geopolitical-cyber-threats.html>
7. <https://www.wired.com/story/petya-ransomware-ukraine/>
8. From article by Grant Elliott, Ostendio CEO, published at: <https://www.darkreading.com/application-security/with-billions-spent-on-cybersecurity-why-are-problems-getting-worse/a/d-id/1328896>
9. <http://ostendio.com/five-tips-culture-cybersecurity/>