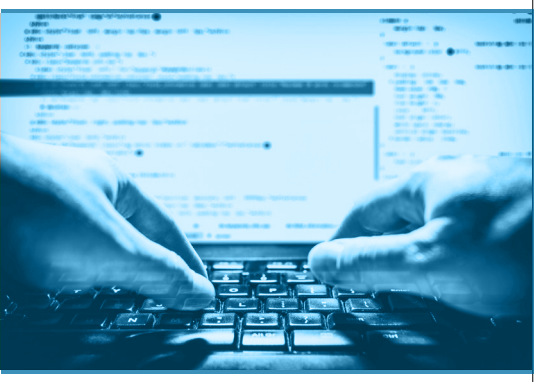
InteliSecure

At a Glance

- Beyond the Hype
- Consider Attacker Motive and Opportunity
- Take the Data Loss Prevention Steps That Matter
- Partnering for Success



What is your risk appetite?

Cybercrime probably affects your business more than you think. Learn how to access data protection strategies that make a difference.

INTELISECURE GUIDE

Putting Cybercrime in Perspective

Cybercrime is big news. It seems almost weekly we see reports of a massive company affected by an even more massive data breach. We hear about the sophistication of the cybercrime economy on the dark web. And we hear politicians ranting about preventing cyberattacks by government-sponsored hackers.

Is it all hype? How much does cybercrime affect YOUR business—really?

Surprisingly, many midsize companies and smaller enterprises often tell us they don't feel they are really a target. They brush off the need for data security by telling themselves a couple of different kinds of stories:

- **We're too small.** After all, we are not Capital One. We hold a modest market share, and we don't have any *real* secrets.
- **There isn't anything we can do about it.** We don't have the resources to do data protection like a giant corporation—how could we possibly prevent a breach?

Those brush-offs are myths. The truth is:

- **Cybercriminals don't care how big your company is;** your data is extremely valuable. (And yes, you do have Intellectual Property (IP) that is worth a lot.)
- **Midsize companies are held accountable** to the same regulatory requirements as large enterprises, so it's essential that you meet those mandates.

To ensure effective, cost-efficient data protection, midsize companies need to put their security needs into business terms.

WHAT'S YOUR RISK APPETITE? CONSIDER ATTACKER MOTIVE AND OPPORTUNITY

To put some perspective around your risk for data loss, don't focus too much on the giant data breaches reported in the media. Instead, consider a criminal's motives and how they take advantage of opportunities.

Say you are a midsize regional hospital. In the gift shop, an employee leaves a $100 bill on the counter during a transaction. That bill is an opportunity; a fast-thinking criminal can snap up the bill and run out. Of course, the risk of getting caught with that $100 is reasonably high.

What if instead the gift shop employees leave an unsecured router on the counter? A thoughtful criminal might recognize that as a greater opportunity. Their motive for stealing data using that router might be to sell employee and patient Personally Identifiable Information (PII)—or it might be just to prove that they can break in. But the theft itself may not be discovered for a long time, and the chance of getting caught is pretty low.

Regardless, you've now lost control of that PII. You have a data breach.

WHAT WILL LOST DATA COST YOU?

According to the Ponemon Institute's 2019 Cost of a Data Breach Report:

- The average global cost of a data breach is $3.92 million.
- Healthcare is the industry with the highest breach costs—averaging $6.45 million.
- In highly regulated environments, costs have a longer impact, spanning more than 2 years.

That kind of impact could be devastating.

TAKE THE DATA LOSS PREVENTION STEPS THAT MATTER

Of course, cybercriminals can access your company's systems and sensitive information through numerous approaches; an unsecured router is just one method. How can you implement data protection in a way that's going to make the biggest impact in the most cost-efficient way?

The Ponemon Institute's *2019 Cost of a Data Breach* report offers recommendations for security program elements that make the greatest reduction in a breach's financial impact:

- **Discover, classify, and encrypt sensitive information,** ensuring the most sensitive data is encrypted on premises, at the endpoint, in transit, and in the cloud.
- **Invest in technologies** that help improve the ability to rapidly detect and contain a data breach, including security automation and intelligent orchestration capabilities that provide visibility across the Security Operations Center (SOC).
- **Minimize complexity** of IT and security environments to make it easier to quickly identify breaches caused by third parties, compliance failures, extensive cloud migration, system complexity, and extensive IoT, mobile, and OT environments.
- **Know how you will identify genuine incidents** and how you will respond to them. Organizations that have developed expertise in responding and remediating security incidents can respond quickly to contain the fallout from a breach.

PARTNERING FOR SUCCESS

Ultimately, investing in a comprehensive data protection program is the best way to manage your risk. Companies of all sizes must be highly aware of their risk tolerance and make informed decisions about how to invest appropriately to provide the level of protection their customers, regulators, and stakeholders demand.

We can't face the future of data protection—and all the challenges of the evolving cybercrime landscape—by working in isolation. Companies need outside input to evolve more innovative and efficient data protection practices.

An experienced data protection provider that combines technical knowledge with an understanding of your business can be advantageous to your security posture. Look for a provider that can offer a broad range professional services to evaluate your current security programs and make technology-neutral recommendations for protecting your critical data assets.

Then, take advantage of an ongoing partnership with a managed data protection service provider. The partner's focused attention and resources can help you continually evolve your security program while protecting against threats to your most critical data assets.

WHERE DOES YOUR DATA PROTECTION PROGRAM STAND?

For any size enterprise, from midsize organizations to large global corporations, working with a trusted managed data protection service provider can help you reduce the risk of data loss.

InteliSecure experts bring more than 15 years' experience in security analysis and data protection strategy. Contact us to discuss your organization's data protection needs—and find the solution that fits.

ABOUT INTELISECURE

InteliSecure specializes in making data protection easy, fast, and cost-effective for companies of nearly every size. More than 500 clients with over 2 million managed users rely on our services and specialists to protect the integrity and safety of their sensitive information. With more than 15 years' experience and partnerships with some of the world's biggest names in cyber defense, we make data security and compliance easy by providing effective data protection at a lower cost, eliminating the strain on IT organizations and reducing the risk of confidential information getting into the wrong hands. Unlike other security providers, we focus on business outcomes—providing data and reports that make sense to business and security executives alike. InteliSecure serves clients globally with security operations centers in the United States and the United Kingdom.

InteliSecure sales@intelisecure.com | www.intelisecure.com

5613 DTC Parkway, Suite 1250 Greenwood Village, CO 80111 | + 1 (720) 227-0990
1 Lindenwood, Chineham Business Park Crockford Lane, Basingstoke, RG24 8QY, UK | +44 118 976 8960