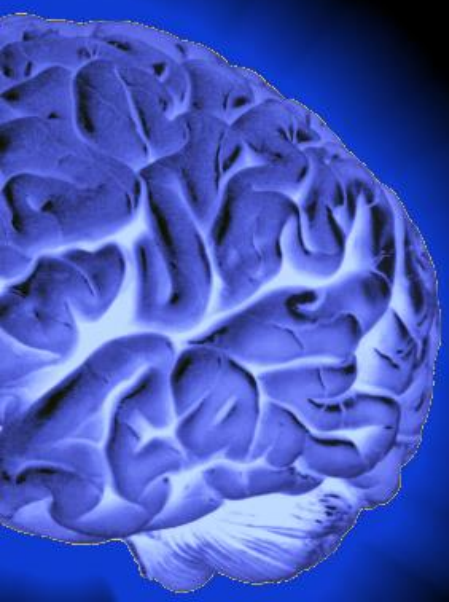


Intellyx White Paper

Don't Let Your Data Center Become a Crime Scene

Charles Araujo

January 5, 2017

Data security is not an abstract idea or just another technical problem – a security breach is a crime and you need to have a digital CSI team

> *The lights flickered as the group entered the cavernous room. Pieces of shattered glass and anodized metal littered the floor. The racks, which should have been standing upright, were on the floor, clearly showing signs of a great struggle.*
>
> *The crime scene investigation team surveyed the situation in the data center. Their job was to figure out just what had happened, who had committed what crimes and most importantly, what it was going to take to catch the crooks and put things back together.*
>
> *At that moment, the chief investigative officer – the CIO, or simply "chief," to her team – walked in and surveyed the crime scene, saying, "OK, team. Run it down for me."*

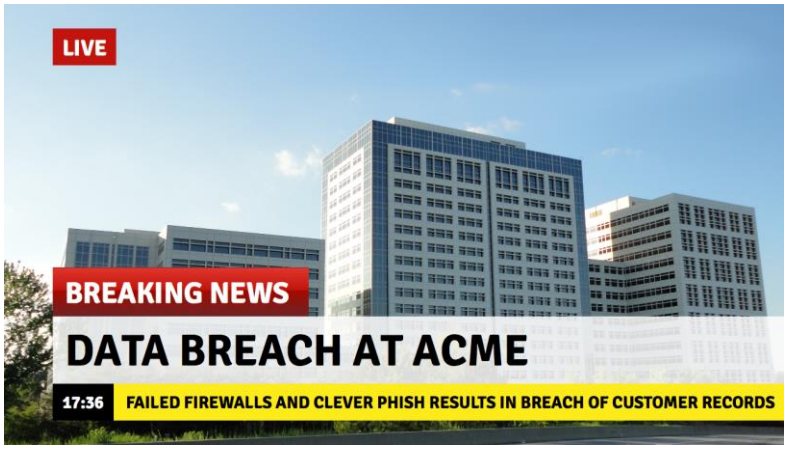
* * *

This story illustrates what it should feel like whenever there is a data breach within an organization. It's a crime scene, and you should treat it like one. And it should be the goal of every CIO and corporate executive to never find themselves in the middle of one – but to be prepared to respond like a CSI team if they do.

The challenge is that there is no physical evidence when a data breach occurs, and the organization may not feel the true ramifications for days, weeks or months. As a result, too many business and IT executives see data security in purely abstract terms and fail to see it for what it is: a crime against your organization.

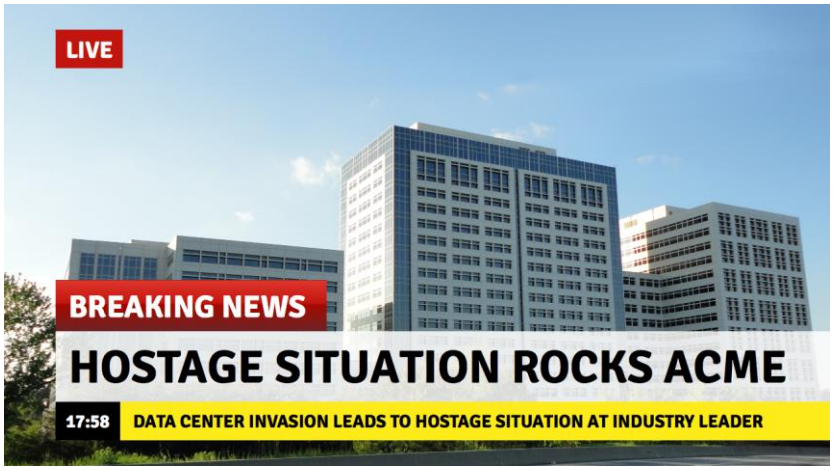
In this white paper, we will examine the risks of viewing data security in purely technical terms, the real impact of data crime on your organization and why you need to take a measured and proactive approach to securing your most vital organizational asset: *your data*.

The Data Center Crime Scene



No CIO or corporate executive wants to wake up to this breaking news story. A data breach is serious stuff – the numerous news stories that break each year being evidence to this fact.

But the truth is that it is becoming so commonplace that it's easy to forget what we're really talking about. What would happen if you woke up to this instead:



When there is a data breach at your organization, this illustration shows what really happened. Organizations need to stop thinking about data security in abstract terms that downplay the significance of the situation. And you need to treat it with the same gravity as if someone had forcibly stormed your data center.

The challenge is that data breaches are, by their nature, a technical issue. There is (generally) no physical break-in. No weapons are involved – physical ones, anyway. So it is easy to forget that a data breach is much more than *just* a technical issue.

Perhaps the best way to think about this is through an analogy. Whether you like it or not, your organization now lives in Internet City. When you moved in, your neighborhood was nice and clean and safe. There weren't many of you, and you all knew each other. You could go about your business without much concern about your security or safety. Life was good.

But over the last couple of decades, your neighborhood has gone downhill – very downhill.

Today, your once quiet, quaint and safe neighborhood is inner-city rough. It's no longer safe to walk down the street – let alone to leave your door open like you once did. You're surrounded by people who wish to do you harm – and as much as you may want to, you can't move away.

Internet City is now your home, so it's time for you to come to terms with your situation and take steps to protect yourself.

Theft, Trespassing, and a Hostage Situation

One of the great dangers of abstracting security issues into simplistic, technical terms is that it obscures the diversity and breadth of the risk.

Rarely does anyone outside of the IT security team discuss any of the specific risks or vulnerabilities to which the organization is susceptible. In the executive suite, the conversation boils down to "information security" or "cybersecurity."

This disconnect is a bit like a big-city mayor only talking about crime in the abstract. It doesn't work. To protect the city and reduce the crime rate requires that you understand what crime is occurring, where it's happening and why a given community is vulnerable to it.

RARELY DOES ANYONE OUTSIDE OF THE IT SECURITY TEAM DISCUSS ANY OF THE SPECIFIC RISKS OR VULNERABILITIES TO WHICH THE ORGANIZATION IS SUSCEPTIBLE.

It's the same when it comes to data security. You need to understand your specific vulnerabilities – in real-world terms – to have any hope of combating them. Some of the major risks you face include:

Grand (IP) Theft

This may come in the form of current or former employees taking intellectual property that belongs to the organization (whether the team realizes it or not). It may also come in the form of external agents using techniques to gain privileged access to your proprietary data. In either case, the result is the same: someone has stolen your valuable IP or other data.

(Digital) Extortion

Ransomware is a catchy term, but its catchiness belies its ugly reality. Using sophisticated techniques, bad actors penetrate your organization's defenses and take your data hostage. They then extort a ransom against the threat that you will never get your data back – and as in real-life hostage scenarios, you often do not.

Indecent (Data) Exposure

Our modern organizations are awash in data – often highly sensitive data. The abundance and prevalence of data, however, has desensitized many on your staff to its criticality and need for protection. As a result, your team may publicly expose important data – often subject to regulation and heavy fines for mishandling – through inattention, carelessness or outright malfeasance.

(Data) Trespassing

Employees may take advantage of your storage assets to store personal, non-organizational data within your environment. Not only is this the unauthorized use of organizational assets (trespassing), it also introduces additional risk in the form malware or similar security vulnerabilities.

* * *

In the real world, and out of a technical context, you would never allow external actors or internal employees to perpetrate these kinds of crimes against your organization. From a business perspective, their impact is just as significant – and you need to take action.

The Real Cost of Data Crime

The costs of data crime are real. According to a recent Kaspersky Lab study, the average hard cost of a single security breach within an enterprise organization is now nearly a million dollars. The study explains that the costs of a security breach are rising because of a combination of the sensitivity of the data being breached and the complexity of the systems hosting it.

As organizations continue to put more and more sensitive and mission-critical data on virtualized systems and in the cloud, the risks continue to multiply. Moreover, as organizations transform

THE AVERAGE HARD COST OF A SINGLE SECURITY BREACH WITHIN AN ENTERPRISE ORGANI-ZATION IS NOW NEARLY A MILLION DOLLARS.

into digital enterprises, they are introducing greater technical complexity into their environments – making it that much harder to secure and protect their data.

The ramifications on both an organizational and personal level are severe. Just ask the leaders of Target, Yahoo, Oracle or the IRS – all of which suffered breaches in the last few years alone. But there is also a reputational cost to organizations.

According to a recent Forbes/IBM report, 46 percent of organizations have already suffered damage to their brand value due to a data breach. It's safe to assume that number will continue to increase.

But the costs of a data breach cannot be measured solely in career or financial terms. There's an even larger, more devastating cost that is less discussed – the impact to your competitive edge.

After a breach to which the response was chaotic and costly, an organization becomes more conservative and risk averse – precisely the opposite of what it needs to be in the digital era. It is clear that this is a challenge organizations must address directly and explicitly.

Simplistic Strategies for a Complex Problem

Despite the real and apparent cost of data breaches, most organizations have taken an overly simplistic and one-dimensional approach to both their defensive strategies and response protocols.

It's the equivalent of buying an extra deadbolt for the front door and hoping it will be enough. Beyond making it a little tougher for someone to come in through the front door, it has virtually no effect.

Undeniably, security is now a top-of-mind problem for every IT and business executive. No one wants to be the next Target or Yahoo. Organizations have therefore offered up budget to try to protect against the threat.

SECURITY IS NOW A TOP-OF-MIND PROBLEM FOR EVERY IT AND BUSINESS EXECUTIVE.

The industry's response is predictable. There has been an avalanche of narrowly focused point solutions rushing to the market to try to seize a piece of the budgetary pie. But far too many of these solutions are overly simplistic, focusing on only a small part of the problem and unable to have any meaningful impact.

Organizations require a more comprehensive approach to security. IT leaders must look at security from a preventative point-of-view and identify vulnerabilities in advance.

Each organization is unique. As a result, the vulnerabilities it faces and the relative risk of any specific data crime is distinctly its own – and demands a corresponding defense and response strategy. This is where simple point solutions go wrong: being narrowly focused, they do not provide organizations with the flexibility they require to respond to such a complex situation.

It is only by taking a comprehensive, holistic approach to data security that organizations can avoid cowering in fear – so that they can instead remain focused on the future.

Securing What Counts: Your Data

The key to this more comprehensive approach is focusing on one thing: *your data*.

With all the talk about security, it's easy to overlook what you're actually protecting. While servers, networks, and other infrastructural elements are important, when it comes right down to it, the only thing that really matters is securing your data. The rest is just a means to an end.

THE ONLY THING THAT REALLY MATTERS IS SECURING YOUR DATA.

Think of it like an expensive coat at a high-end retailer. Yes, you want security cameras, strong doors, and reliable locks. They help keep the wrong people out, but that's not enough. You also need to secure the coat itself (like those little security devices on items at Nordstrom).

You need to be able to keep track of your data in motion and through state and location changes. That next layer of protection secures your data from those that get through the outer defenses and from internal perpetrators.

In truth, protecting data is much more complicated than protecting a coat at a high-end retailer. Unlike a coat, a criminal can replicate, move, change, corrupt, lock or otherwise corrupt your data. That means protecting your data is much harder and demands a significantly higher level of attention.

But the challenge is even more complex. In the event an attacker compromises your data in some way – which is almost inevitable, no matter how robust your security strategy – you need to be able to restore it as quickly and with as little impact as possible.

That restoration is no trivial matter.

According to a recent study by Experian, enterprise organizations estimate that it takes between 8 months and a year to recover from a significant data breach, in terms of both reputation and operational capability. An organization's ability to both protect against a breach and its ability to rapidly recover from a breach, therefore, must be equal parts of their data resiliency strategy.

Moving Faster Than the Speed of Fear

The need for speed and agility is a must-have in the digital era. Move too slow, and you won't survive, what Intellyx calls the *opportunity risk inflection point*: when the risk of *not* transforming traditional IT surpasses the risks inherent in moving forward with such transformation. But fear of a security breach paralyzes too many organizations.

They recognize the risk and scramble to protect themselves only to find that they have employed overly simplistic and too narrow solutions. Too late, they discover that they have not addressed security holistically or focused on what matters most: their data.

In the end, the inevitable breach occurs and they then scramble to determine the extent of the damage and how to recover from it.

But there is another way.

Organizations must see their data center as a potential crime scene. You must look at your data landscape holistically and then employ data-centric techniques, such as those DataGravity offers, to both protect your data and ensure that you can rapidly recover in the event of a breach.

YOU MUST LOOK AT YOUR DATA LANDSCAPE HOLISTICALLY AND THEN EMPLOY DATA-CENTRIC TECHNIQUES, SUCH AS THOSE DATAGRAVITY OFFERS, TO BOTH PROTECT YOUR DATA AND ENSURE THAT YOU CAN RAPIDLY RECOVER IN THE EVENT OF A BREACH.

As the digital era continues to evolve, it is becoming increasingly clear that nothing is more important than your proprietary data and intellectual property. You need to see its protection as more than an abstraction or a purely technical problem. You need to accept the mantle of the other CIO – the chief investigative officer – to see your data from all angles and prepare for whatever may come.