Heading 1: **Cyber Security in Crisis**

Sub: *Lessons from high-profile data breaches.*

Heading 2: **Corporate Compliance and Cybersecurity**

Sub: *What can data breaches teach us?*

Heading 3: **Is Data Theft a Preventable Debacle?**

Sub: *You are only as good as your weakest link.*

Looking back, 2017 could go down as the year cybersecurity failed. One study revealed 918 recorded data breaches in the first half of the year, resulting in a "staggering 164% increase over the last six months of 2016."

Image

The Equifax Data Breach was unmatched in the type of data compromised and the number of affected individuals. But although it may have been the “biggest,” it probably won’t be the last. The veritable flood of data hacks across big business have exposed major flaws in the way companies “lock the door” against intrusions.

Data is the lifeblood of the modern business – arguably its most important asset. Building a solid data security strategy should be every organization’s priority, but a disturbing number of companies are barely fulfilling compliance requirements.

How far must organizations go when closing the door on vulnerable data? As it turns out, not far. All too often, data breaches are proven to be the fault of ineffective and slipshod risk management. And that means they are preventable.

Safeguarding the Systems

The phrase "there's no such thing as perfect security" is well known in the computer security industry. IT security experts believe that effective security can be enhanced by information audits, something organizations shy away from because of the costs involved.

But the issue isn't always with the system. There’s the problem of human error; the people that work with the systems and data – a factor that has been implicated in nearly every major data breach.

The problems escalate when risk management fails to effectively monitor processes.
In its most recent Risk Alert, the Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) cites the following elements of a robust cybersecurity program:

- Maintenance of an inventory of data, information, and vendors
- Detailed cybersecurity-related instructions
- Maintenance of schedules and processes for testing data integrity and vulnerabilities
- Establishing and enforcing controls to access data and systems
- Mandatory employee training

- Engaged senior management

Data breaches are inevitable, but they can be prevented or minimized. How organizations prepare and react to them is crucial.

Image

Assess the Risk

Organizations need to assess their cybersecurity as well as risk severity. In many cases, companies do not know the assets they have or where vulnerabilities exist.

Tips for a great briefing include:

- Outlining where cyber vulnerabilities exist
- Proactively managing cybersecurity risks

- Prioritizing IT vulnerabilities to decide which ones to address first
- Developing and applying actionable and comprehensive risk mitigation strategies
- Applying data in support of cybersecurity compliance and audit requirements
- Continuously monitoring IT assets for cybersecurity risks

GDRP and Cybersecurity

The General Data Protection Regulation (GDPR) comes into effect in May 2018. As a result of recent prominent data breaches, multinational companies operating in Europe will have to comply with the new standards.

The main objective of the GDPR is to reduce substantial data breaches in the EU. As such, the legislation sets a high standard for data protection in other nations. New GDPR standards will better prepare businesses to evade data breaches. But in the evolving landscape of cybercrime, no system or standard can be foolproof.

Image

The Takeaway

By giving untrained and unmotivated individuals access to corporate data systems, organizations leave the door wide open for data breaches. Companies need to encourage robust vigilance at every level of the data chain.

Massive security breaches are a danger to any organization. Data failures damage clients' loyalty and compromise the integrity of a business's reputation. Protect your business from the fallout created by cyber crime. Conduct continual risk assessment, stay on top of new regulations, and emphasize adherence to proactive compliance.