

EBOOK

Are CEOs Responsible for
Their Companies'
DATA BREACHES?



Many believe they are – primarily due to **7** overlooked security standards & **7** negative behaviors.

Most executives in businesses both large and small are confident that they are well prepared for cyberthreats when they're not. This in itself is a huge risk. They believe that because they've increased investments in cybersecurity that their data is safe.

Their confidence is misplaced – why is this?

Because they often overlook 7 well-known security standards:

1. Security policies must be consistently applied.
2. Ongoing user security awareness training must be a priority.
3. More than basic security solutions must be used.
4. Regular vulnerability assessments testing and reporting is essential.
5. If a breach does occur, changes to security policies and practices must be implemented.
6. Defense-in-depth prevention techniques must be deployed.
7. 24/7 remote monitoring for malicious threats and mitigation is a must.



DO YOU BELIEVE CEOs ARE TO BLAME FOR SO MANY OF TODAY'S SECURITY EVENTS?

These misinformed individuals are often overconfident in their organization's ability to tackle specific threats. For example, they are "sure" that if a mobile device were stolen that they would know what data was on it and be prepared for the level of risk to their business. They are also "sure" that they have what they need to protect their customers' and employees' personally identifiable information.

It's no wonder the number of data breaches is reaching epidemic proportions. It seems like every few weeks we learn about another devastating security breach that strikes a large corporation – and, we're not even hearing about the smaller ones. If CEOs and business leaders aren't informed when it comes to the security posture of their businesses, can we trust our private information with them? This shortsightedness and complacency borderlines on neglect.


**According to
Juniper Research,
cybercrime is on the
rise and will cost
businesses \$2.1
trillion by 2019.**



Take the Equifax breach for example:

Equifax alerted the public in September 2017 to a massive data breach that exposed the personal and financial information, including names, birthdays, credit card numbers and Social Security numbers, of approximately 145 million customers in the United States to hackers. Following the Equifax breach, the former CEO Richard Smith and the current interim CEO Paulino do Rego Barros Jr. were called to testify before the Committee on Commerce, Science, and Transportation this week for a hearing titled *"Protecting Consumers in the Era of Major Data Breaches."* **During the hearing, Sen. Cory Gardner (R-Colo.) questioned Smith and Barros about Equifax's use of, or lack of, encryption for customer data at rest.** Smith confirmed that the company was not encrypting data at the time of the Equifax breach, and Gardner questioned whether or not that was intentional. *"Was the fact that [customer] data remained unencrypted at rest the result of an oversight, or was that a decision that was made to manage that data unencrypted at rest?"* Gardner asked Smith. Smith pointed out that encryption at rest is just one method of security but eventually confirmed that a decision was made to leave customer data unencrypted at rest. *"So, a decision was made to leave it unencrypted at rest?"* Gardner pushed. *"Correct,"* Smith responded.

In their *"2016 Cost of Data Breach Study: Global Analysis,"* IBM and Ponemon calculated a standard cost per loss of a stolen record of to be \$158. This number includes direct and indirect expenses, such as remediation and in-house investigations. It also includes the value of damage to the brand, and loss of current as well as future customers.

A hand is shown pointing at a glowing target with concentric circles. The background is dark with binary code (0s and 1s) floating around. The target is bright and has a purple glow.

CAN A CEO'S OVERCONFIDENCE LEAD TO A DATA BREACH? IT APPEARS THE ANSWER TO THIS QUESTION IS YES.

The following are 7 behaviors that CEOs exhibit which are directly related to the increasing incidence of data breaches.

1. Inconsistent Enforcement of Security Policies

Security policies are worthless unless they are practiced and strictly enforced. Sometimes what happens is that while one executive designs security solutions another executive checks the security of the design, and yet another oversees company security. There are gaps in this system that allow hackers to gain access to information.

Security experts insist that employees must be exposed to a security policy five times before they understand its importance and practice it. They stress the importance of making policies easily accessible and conducting periodic cybersecurity awareness training.

A hand is holding a smartphone. On the screen, there is a red button with the text 'Data protection' and a password field with five asterisks. A red banner at the bottom of the phone contains the text 'Does your organization practice and enforce your IT security policy?'.

Does your organization practice and enforce your IT security policy?

Employees should know and understand that if they violate cybersecurity policies what punishments they can face. Enforcement must be consistent but doesn't need to be extremely punitive. If an IT department discovers an infraction, they can block the prohibited activity with firewalls, router blacklists and content filters. This way the violation remains private and a manager can quietly discuss the problem with the employee. The severity of the punishment should reflect the degree of the violation. Unfortunately, in some cases, this means an employee must be terminated.

Most CEOs try to hide employee dismissals due to security policy violations. However, as data breaches increase, and regulations like FINRA and HIPAA result in businesses facing severe consequences, more are recognizing the need to use dismissals as an example for other employees.

2. Some CEOs are negligent when it comes to providing Security Awareness Training for employees.

This is because developing a cybersecurity awareness program isn't easy. However, providing employees with regular training and ensuring they understand and follow security policies, is an important piece of data security.

If employees don't know or understand how to recognize cyber threats and maintain the confidentiality of data, it's usually the fault of the CEO who disregards the importance of training. By doing this, they risk damage to their business and valuable data assets, as well as their corporate reputation.

Laws under the U.S. Federal Sentencing Guidelines require some form of training and awareness activities to prevent data breaches. CEOs must ask themselves the following:

- How frequently and how well does the organization communicate its policies to personnel?
- Are personnel getting effectively trained and receiving awareness?
- What methods does the organization use for such communications?
- Does the organization verify that the desired results from training occur?
- Does the organization update the education program to improve communications and to get the right message out to personnel?
- Does the training cover ethical work practices?
- Is there ongoing compliance and ethics dialogue between staff and management?
- Is management getting the same educational messages as the staff?

3. Many CEOs are shortsighted when it comes to the application of cybersecurity technologies.

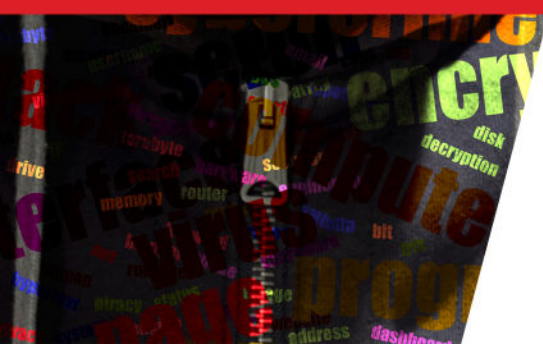
Research from the 2017 State of Cybersecurity Metrics Report reveals that:

- One in three companies invests in cybersecurity technologies without any way to measure their value or effectiveness.
- Four out of five companies don't know where their sensitive data is located, nor how to secure it.
- Four out of five companies fail to communicate effectively with business stakeholders or include them in cybersecurity investment decisions.
- Two out of three companies don't fully measure whether their disaster recovery will work as planned.
- Four out of five never measure the success of security training investments.

**The Verizon
2016 Data Breach
Investigations
Report states
that no location,
industry or
organization is
immune from
attack.**



**Sixty percent
of CEOs don't
adequately protect
their business's
privileged accounts.**



4. Many CEOs are complacent with it comes to vulnerability reporting.

Only a small percentage of companies can say that their vulnerability reporting is robust, and many don't have plans or processes to do this. Vulnerabilities are often discovered years after they are introduced, and usually after a breach has occurred. CEOs need to stay on top of the gaps in their data security systems and contract with IT professionals to implement regular Vulnerability Assessments and Deep Scan IT Audits. For their businesses to be totally secure, CEOs and managers must stay on top of the vulnerabilities affecting their networks and applications.

5. Some can be inflexible to changing processes after a data breach.

In a study by SolarWinds, only 44% of CEOs implemented new technology after a data breach. And according to the Federal Trade Commission, this is a must. You must fix your vulnerabilities, which in most cases means adopting newer, more robust technologies. *"Find out if measures such as encryption were enabled when the breach happened. Analyze backup or preserved data. Review logs to determine who had access to the data at the time of the breach. Also, analyze who currently has access, determine whether that access is needed, and restrict access if it is not. Verify the types of information compromised, the number of people affected, and whether you have contact information for those people. When you get the forensic reports, take the recommended remedial measures as soon as possible."*

Small businesses are targeted in two out of three cyber attacks.

6. CEOs can remain stagnant in the application of key prevention techniques.

Many don't align data protection with their company's changing goals. When this happens, security measures are less effective and become outdated as they are no longer the right fit for a growing business. You should be working with a vCIO from a reliable IT provider in Atlanta. They will get to know your business, your short and long-term goals, and help you install and implement the best security technologies to meet your growing business needs.

7. CEOs can often become lethargic when it comes to cyber-threat detection and response.

With hackers employing techniques that are more sophisticated than ever, CEOs must find solutions that employ a holistic approach to network and endpoint security. Again, all it takes is the assistance of a professional who is certified in the latest cybersecurity solutions. When CEOs have a trusted IT partner, they can focus on their business rather than IT security.

For more information, contact Amnet – The IT Department for Your Business.



COLORADO SPRINGS

(719) 442-6683 / 219 W. Colorado Ave., Suite 200, Colorado Springs, CO 80903

DENVER

(303) 825-3228 / 110 16th St., Suite 1400, Denver, CO 80202