**GOVERNOR ERIC J. HOLCOMB'S**
**INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

---

Ridge, Tom & Lazio, Rick

"Why Cybersecurity must be a top priority for Small and Midsize businesses"

Darkreading.com

informa tech Technology Group

24 January 2019

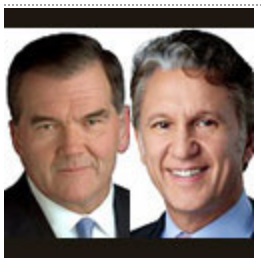
**URL:** https://www.darkreading.com/attacks-breaches/why-cybersecurity-must-be-a-top-priority-for-small-and-midsize-businesses--/a/d-id/1333700

**Accessed:** 02 July 2019

**Synopsis:** The big corporations may grab the headlines, but America's SMBs have the most to lose in the aftermath of a data breach.
This is the new reality of the digital world, and public and private entities- from government agencies to multinational corporations to small and midsize businesses – must be prepared to place higher priority on implementing cybersecurity measures.

DARKReading

1/24/2019
10:30 AM



Tom Ridge & Rick Lazio
Commentary
Connect Directly



# Why Cybersecurity Must Be a Top Priority for Small & Midsize Businesses

**The big corporations may grab the headlines, but America's SMBs have the most to lose in the aftermath of a data breach.**

From Equifax to Under Armour to the recent news from Marriott, it seems that every week brings a new headline regarding a major data or security breach. The Marriott hack is just the latest in a long line of high-profile cyberattacks, with the hotel giant revealing that a massive breach exposed the personal data of more than 500 million customers.

But though the big corporations seize the cyberattack headlines, America's small and midsize businesses may have even more to lose when it comes to the ramifications of a breach. From the immediate damage (both financially and in terms of hours of lost productivity) to the lasting harm to a company's reputation and brand credibility, the stakes for cybersecurity have never been higher for smaller businesses. According to the US National Cyber Security Alliance, an estimated 60% of small companies will go out of business within just six months of a cyberattack, illustrating the real-world consequences of inadequate cybersecurity measures.

As technology advances, so will the prevalence and scope of cyberattacks. Every day, the Internet of Things (IoT) is making our world more interconnected, with an estimated 20 billion IoT devices expected to be deployed by 2020. With this increased connectivity and greater reliance on mobile technologies come additional points of vulnerability — and the potential for greater damage from cyberattacks launched by criminals, nation-states, and other bad-faith actors.

## The Risk for Small and Midsize Companies

This is the new reality of the digital world, and public and private entities — from government agencies and multinational corporations to small and midsize businesses — must be prepared to place a higher priority on implementing cybersecurity measures.

In the case of small and midsize businesses, statistics show that they are not only just as vulnerable to a breach, but the consequences of such an event can be downright catastrophic. According to data gathered by the Ponemon Institute, the percentage of small businesses that have experienced a

cyberattack climbed from 55% in 2016 to 61% in 2017. In Verizon's 2018 Data Breach Investigations Report, 58% of malware attack victims were categorized as small businesses.

The most alarming statistics, however, relate to the potential monetary and long-term impact of a breach. The Ponemon study notes that in 2017, the average cost of cyberattacks on small and medium-size businesses was more than $2.2 million, with malware-related costs averaging more than $1 million in damages or theft of IT assets and more than $1.2 million as a result of the disruption to business operations. Those are staggering numbers — and they help explain why an estimated 60% of small companies go out of business within six months of a cyberattack.

**How to Protect Yourself**

Given the high stakes that come with a potential breach, small and midsize businesses can take steps to protect their most vital and confidential information. To start, organizations must have a cybersecurity plan in place that will protect their assets and maintain the profitability of the business. Here are three recommendations for building out broader cybersecurity protocols:

- **Have a cybersecurity audit performed by an outside source.** Even if you are confident that your IT department has the organization covered, there are major benefits to having another set of eyes that are divorced from the daily processes of your business to evaluate potential vulnerabilities within the organization. While security and technological performance are both tied to IT, having an experienced cybersecurity professional devoted to just the security aspect may reveal unforeseen vulnerabilities.
- **Create an organizationwide policy that fits the unique needs of your business.** There is no one-size-fits-all approach when building out preventative cybersecurity measures and recovery protocols. This means each organization must sit down and identify what companywide information is invaluable to the business, where it is located, how potential hackers could gain access to this information, and what measures could be put in place to prevent or mitigate the damage of a cyberattack.
- **Implement awareness programs that emphasize the importance of proper "cyber hygiene."** Maintaining the digital security of an entire organization extends far beyond technology and firewalls. Human error often plays a significant role in a breach. Every employee, from the C-suite down, is responsible for exercising good judgment and following companywide cyber protocols. As such, implementing employee training programs is a critical way of informing and reminding employees of potential threats.

Bottom line: Investing in cybersecurity will protect the clients and IP revenue, and create business resilience, thus securing the future of your business.

**Related Content:**

- 2019 Attacker Playbook
- Shadow IT, IaaS & the Security Imperative
- The Security Perimeter Is Dead; Long Live the New Endpoint Perimeter

*Tom Ridge, former Secretary of the U.S. Department of Homeland Security; Chairman of Cybersecurity and Technology, alliantgroup Tom Ridge served as the nation's first Secretary of Homeland Security, leading an agency of more than 180,000 employees responsible for ... View Full Bio*

Ransomeware: To Pay or Not To Pay?

451 Business Impact Brief: Security for Cloud-Native Compute Will Be Different

**MORE WHITE PAPERS**

**Reports**

We Need You: cloud usage & optimization strategies

Salary Survey: Can you spare 10 minutes?

**MORE REPORTS**