TOP EXCUSES

FOR

IGNORING

CYBERSECURITY

HEALTH TECH ACCESS ALLIANCE
2019
INFO@HTAALLIANCE.ORG
301-200-9776

TRULY, AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE.

- Benjamin Franklin

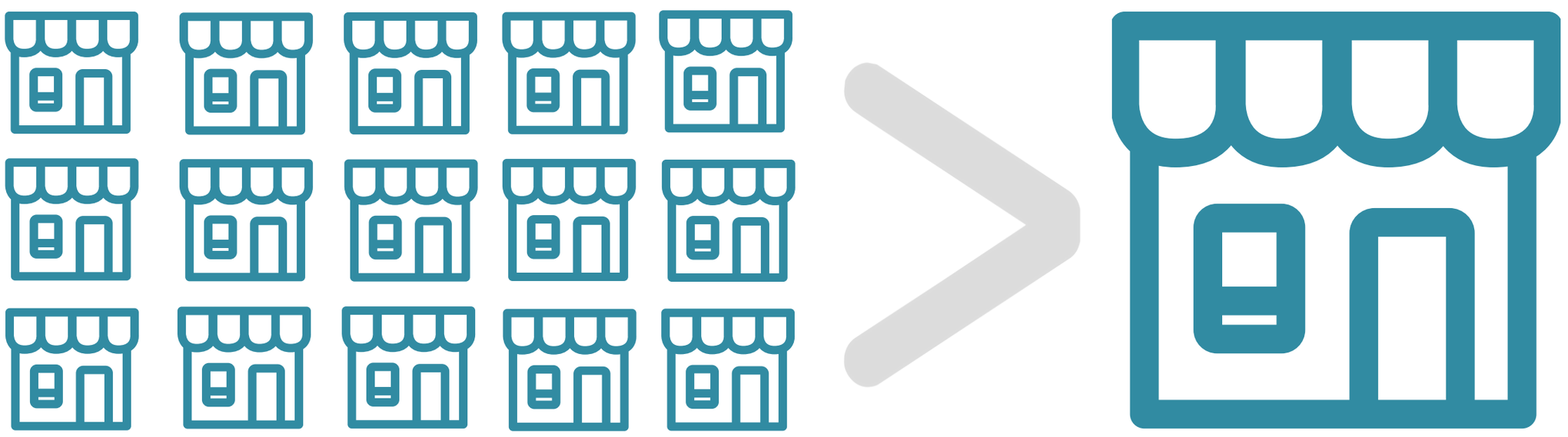
Introduction

We've worked with nearly every type of organization to help them defend from cyber attacks. In trying to get organizations prepared for modern threats, we have seen a number of excuses used by leadership to avoid the problem. Inevitably, these organizations come back to the table, paying much more for an incident response when a dose of prevention would have saved everyone time, money, and stress. This article addresses the top reasons given by future cyber attack victims. For all of these excuses, the question of an attack is not if it will happen, but when.

1. "I'm too little."

The leadership of many small businesses makes the argument that their organization is too little to be of interest to hackers. They argue that their digital footprint is too small and their bank accounts or personal data are not worth the cost for a hacker.

In reality, the small business market makes up a large portion of US GDP. Reports from SBA.gov claim that over 50 percent of the private nonfarm GDP came from small business in 2016. For hackers, it is significantly easier to target 400 small businesses than it would be to find the one chink in the armor of a major company. Tools like www.shodan.io make it easy for hackers to scan entire blocks of the internet for vulnerabilities without regard for the size of the organization.



Larger organizations tend to have better security. The Target security breach required highly specialized hackers to infiltrate an air conditioning system and then specialized knowledge on how to pivot from the air conditioner into the credit card databases. Hackers without these specialized skills rarely find success targeting major corporations.

"When hackers look at potential targets, the fact that an organization is small makes them an easier target, not a harder one."

Instead, they spend their time on less sophisticated hacks, regularly targeting small businesses. Small businesses, from the hacker perspective, are the low hanging fruit.

For the less skilled hacker, these attacks are high risk and highly unlikely to be successful. Much better than, for the novice hacker, to hone his skills with smaller thefts against the myriad of small businesses who refuse to look at cybersecurity. When hackers look at potential targets, the fact that an organization is small makes them an easier target, not a harder one.

Source: https://www.quadmetrics.com/blog/posts/small-business-cybersecurity

2. "It's too hard."

Much of the institutional resistance to looking at cybersecurity comes from the perception that it is difficult to get started. Organizations regularly dread that implementing cybersecurity practices will cost months in time and will rely on esoteric processes which can't be understood by business leadership.

Cybersecurity has matured to the point that it incorporates into other businesses processes. To highlight this, the very first section of the primary industry certification (CISSP) is all about business processes and not about the nuances of hacking.

"SECURITY IS BEST IMPLEMENTED AS EARLY AS POSSIBLE."

The rise of the Chief Information Security Officer (CISO), whose principal task is to integrate cybersecurity into business processes, show how top talent is as comfortable in the boardroom as they are behind a server rack. For organizations too small for a dedicated CISO, many solutions offer remote CISOs and remote security monitoring solutions which simplify the process for today's business leaders.

Further, security is best implemented as early as possible. Security should scale with an organization's growth. Whatever difficulty there is in implementing security only increases as the topic is ignored and insecure organizations grow. It is far easier to start a security program when the organization has five machines, and far more difficult when they have 500. Delaying this task is a recipe for increased risk and complexity.

3. "It's too expensive."

Many organizations looking for security solutions shudder the price tag, and stop looking before the subject has been fully defined. These organizations see five or six-digit price tags from the major cybersecurity organizations and come to the conclusion that they cannot afford to invest in the topic.

In reality, these major cybersecurity organizations only scratch the surface of what is possible. A full enterprise suite of solutions from a major industry player may not be correct for smaller organizations. Whole suites of products are designed and targeted to specifically address this concern. Staff training on cybersecurity basics, initial security scans, and remote network monitoring can cost hundreds, not thousands of dollars and most cybersecurity solutions and/or consultants will work with customers to keep the price tag within budget.

AVERAGE COST PER RECORD

$380

IN HEALTHCARE

Whereas the cost of a breach can look like...

$7
Million

Average cost per breach

89%

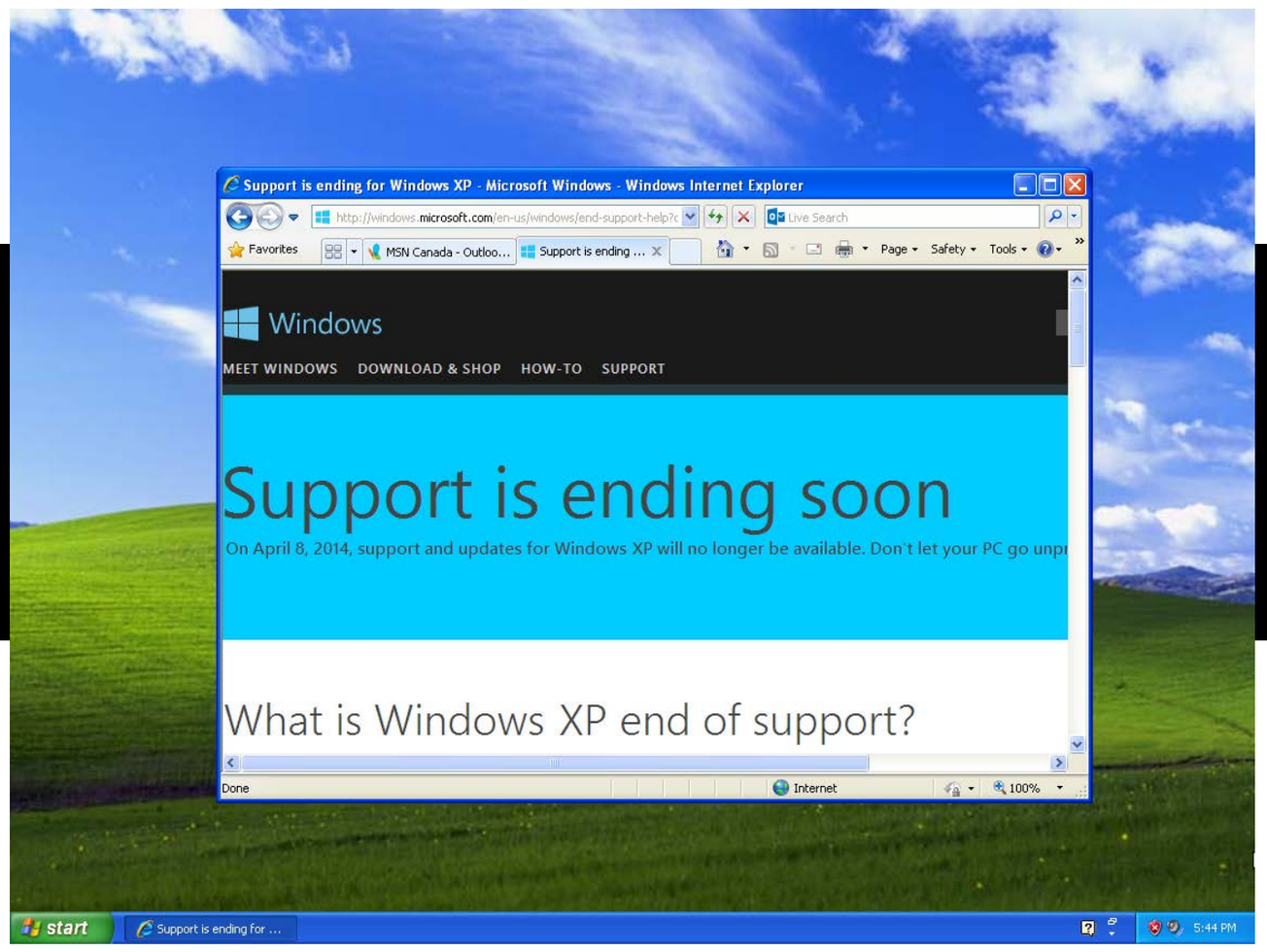
Percent of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past 24 months

20
%

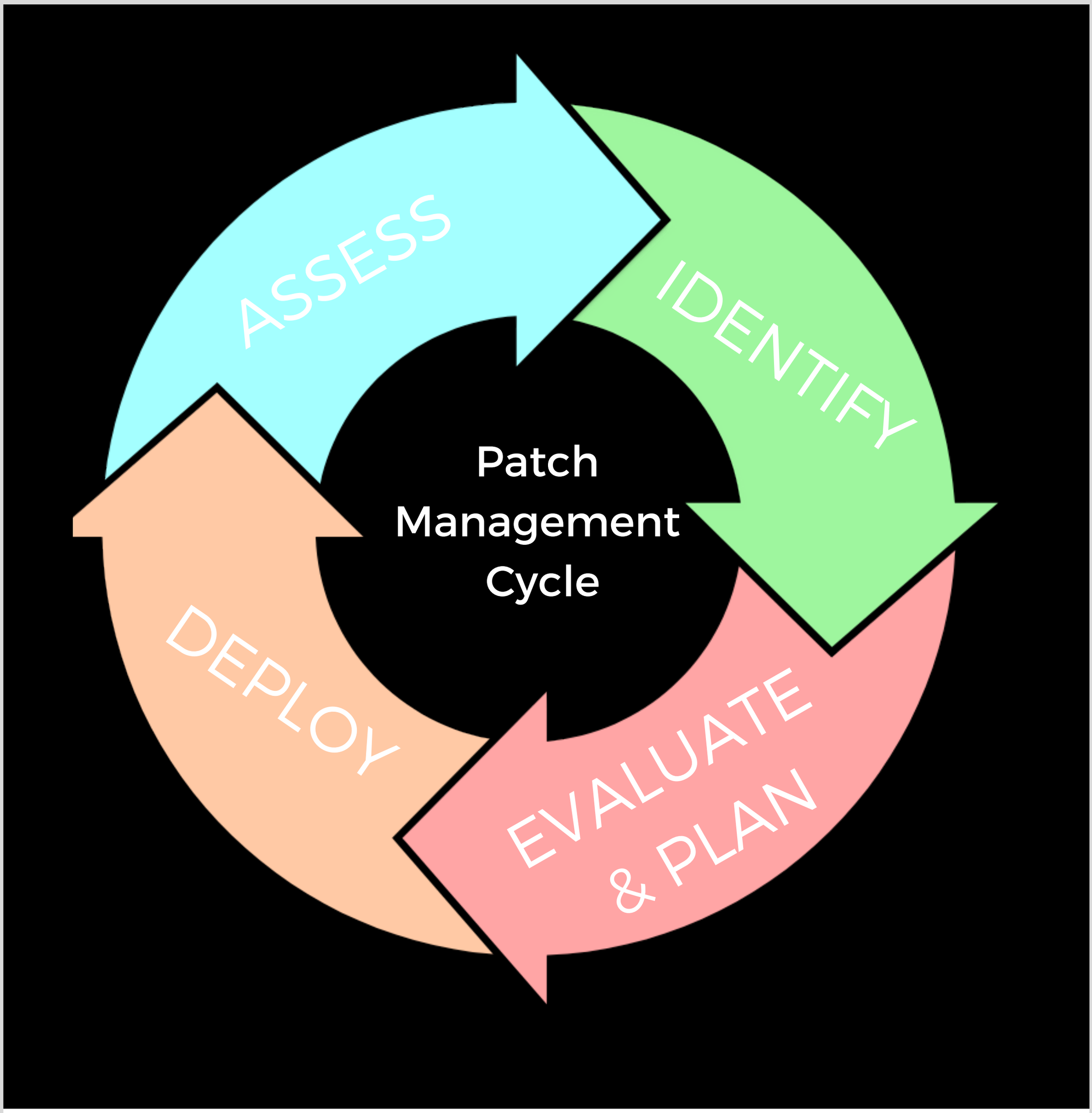
Average loss of revenue following a data breach

4. "It might break the system"

Many organizations with part-time or 3rd party IT staff make the argument that updating business critical processes has the risk of breaking the system and causing expensive outages. Far more than any of the other excuses addressed here, these organizations have a point! As layers of technology chain together, updating one item in the chain may cause system failures further down that chain. An update to a database may crash a website or cause other systems to fail completely. Companies may find that Operating System updates cause older versions of their business-critical software to fail to load. These are real concerns. Famously, the update from Windows XP to Windows 7 caused a large number of major systems, some of them critical to the economy, to fail.



However, the threat of not updating is greater than the risk of business failure, and the industry standard “Patch Management Cycle” mitigates this threat. The failure to address this risk is systemic and hugely costly. Despite Windows XP being so old that Microsoft stopped supporting it in 2014, it remains the third most popular operating system in the world. All of these systems, once connected to the internet, prove to be easy targets for even the lowest level hackers. The same is true for Windows 2003, which hasn’t received updates since 2015 and which Redmond Magazine reported to still be in use by 18% of the market one year later.



The “Patch Management Cycle” is the industry term for the business process which balances the risk of breaking internal systems with the risk of not updating these systems. Reasonable patch management processes will test updates, correct for any errors, and keep any projected downtime away from critical business processes. Without these controls in place, organizations are almost certain to become the victim of a passing hacker.

Cost of Breach Must Be Greater Than Risk of Internal Systems Breaking

5. "Compliance is Enough"

Organizations often specifically request security scans which "check the compliance box" and specifically ask that security teams not look any further than compliance demands. The scans, they argue, are to meet industry compliance standards. Further, they suggest that any additional scans would obligate the organization to add controls for vulnerabilities found beyond those addressed by compliance standards, adding undue cost to their organization. This "head in the sand" approach is the type of thinking which allows vulnerabilities to go unnoticed, and for hackers to sit inside systems for years as auditors continue to bless off on "compliant" systems. It is this type of thinking which has resulted in some of the most devastating hacks we've seen in the media.

Compliance is not security.
Compliance is a check on security.

Compliance is not security. Compliance is a check on security. Being merely compliant is not the same as being secure. Competent risk modeling is as necessary for cybersecurity as it is in any other business function. Business leaders need to know what the risks are, in terms of dollars and cents, in order to identify what risks can safely be absorbed and which risks must be addressed immediately. Working just to meet compliance standards is to not acknowledge the full risks present for an organization and to not plan for those un-acknowledged risks. This is as true in cybersecurity as it is for any other business processes. Compliance checks security, it does not define it.

Food for Thought: How often do you find that regulation is AHEAD of the curve?

6. "3rd Party Providers do it for me."

Some business leaders feel like they've resolved all of these issues with 3rd party security providers. "I have people monitoring these issues for me, I don't need to know anymore," they state.

Ultimately, the success or failure of any business should rest with the decisions of that businesses leadership. Often, great third-party tools are deployed, but with no one inside the organization checking to ensure the solutions were properly implemented. In one ransomware case, the offsite third party providing network monitoring was found to knowingly be covering only a portion of the network devices. Hackers simply attacked all the machines not covered by the third party, crippling the client's network and costing millions of dollars in lost productivity. Leadership needs to know how to verify the effectiveness of third parties and keep them honest. External assessments, periodic reviews, and basic security literacy are all tools which can help ensure that the third parties are doing what they say their doing.

Conclusion

Given enough time and motivation, organizational leadership will always come up with an excuse as to why they aren't secure. Ultimately, excuses won't stop the loss in productivity, customer trust, institutional prestige, and the financial loss suffered from a cybersecurity incident. Leaders should be thinking about security the day an organization is created and should implement reasonable business risk management practices wherever business risk presents itself. Truly, an ounce of prevention is worth a pound of cure. Failure to do so may be the deciding line between those that become leaders of their industry, and those that fall victim to the dustbin of history.

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."
– Bruce Schneier

Health Tech Access Alliance is here to help.

With our expertise and experience, we can provide our QI Express solution, technical assistance and coaching to make sure your Community Health Center, Federally Qualified Health Center, HCCN, or HIE has the tools and expertise to successfully navigate cybersecurity threats and prevention.

HEALTH TECH
ACCESS ALLIANCE

Health Tech Access Alliance
www.htaalliance.org
301-200-9776
security@htaalliance.org