How to be a

Cybersecurity Sentinel

10 Insights for C-Suite Executives

Although cybersecurity has gained national attention in the wake of several high-profile breaches, many hospitals and health systems are unprepared to defend against well-organized and well-funded cyber criminals. Cyber resilience requires improved technology solutions, but leading organizations approach cybersecurity efforts holistically—which starts with having an engaged C-suite and board that share in accountability for protecting the organization. Here's what senior health care executives need to know—and do—to achieve cyber resilience at their organizations.

What you need to **KNOW**

Cyber criminals see health care as **low-hanging fruit**

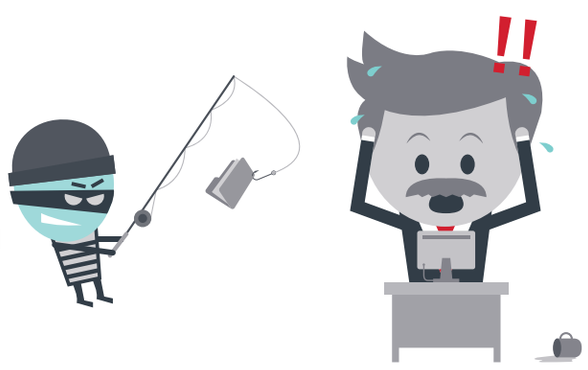
A medical identity is uniquely comprehensive. It's also irreplaceable, making it more valuable than a credit card or even a social security number. Given the health care industry's reputation for using outdated technology and lacking robust security protocols, providers can seem like easy targets.

Cyberattacks lead to **financial, operational, and reputational losses**

In addition to the direct cost of recovery efforts, an attack can lead to a wide range of potential fines and settlements. Organizations may be forced to reschedule or cancel existing appointments, and negative media attention can keep future patients away. All told, costs can range from tens of thousands to hundreds of millions of dollars.

CXOs are held personally responsible when breaches occur

Accountability extends far beyond the IT department. CEOs, CFOs, and board members have been fired following major cyberattacks. And class action lawsuits are directed at the organization—not the IT department.



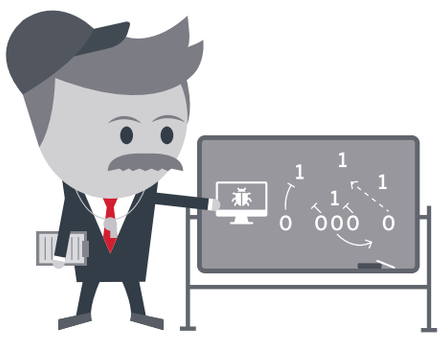
Technology is a necessary, **but insufficient,** part of the solution

It can be easy to think of cybersecurity as a technology problem that needs a technology solution. But leading organizations focus on cybersecurity governance, policy, process, and education to complement their technology and services.

The ultimate goal is to **mitigate—not eliminate**—cyber risk

Total security is impossible to achieve. Instead, every organization must determine its own acceptable level of risk and develop an approach to mitigating risk that aligns with the culture of the organization.

What you need to **DO**



Be a **good partner**

Coordinate with IT leaders to prep for high-stakes meetings and training sessions. Help them refine language and avoid jargon. And assure them that they'll have an ally both inside and outside of the boardroom.

Stay focused and avoid the blame game

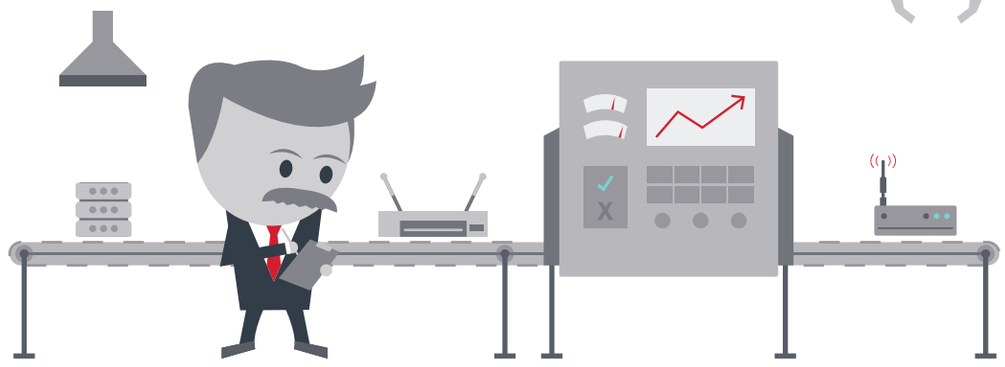
Cybersecurity is a growing issue across many industries, so top talent is hard to find. Finger-pointing is a great way to lose both talent and momentum. Instead, leading organizations hold all employees—non-IT, IT, and executives alike—accountable for risky cyber behavior that endangers patients.

Refine your **partnership and vendor strategies**

Vendors and partners magnify an organization's risk profile. Unfortunately, the public does not easily discern a vendor's role in a breach. Ensure security is part of the due diligence process; have a set of minimum standards and stick to them.

Hardwire training and testing—and repeat frequently

Repeated testing can dramatically decrease failure rates—but 27% of surveyed hospitals never test whether their staff can be fooled by stealth attacks. It is critical to develop an education strategy that includes both training and frequent end user testing.



Lead by example

Make it clear that cybersecurity is a top priority. Leading organizations have C-suites and boards that set aside time for security-related issues, actively participate in training and testing, and aren't afraid to ask questions or admit when they've failed a training test.

Want more support understanding how to confront today's most pressing strategic issues? Expert-led onsite presentations are included with your membership. Learn more at:

advisory.com/hcab/onsites