How companies can stay ahead of the cybersecurity curve

March 21 2017, by Scott Shackelford

Credit: AI-generated image (disclaimer)

If you're like me, on a given day you interact with a whole range of connected technologies for work and play. Just today, I used Box to share and download files for work, called up Tile to find my keys, relied on Google Maps to run an errand while streaming a podcast to my AirPods, and connected via Skype with a colleague overseas. And that

was all before lunch. As we interact with technology of all sorts, what security safeguards should we expect from the companies building the Internet of Everything?

Cyberattacks can interrupt business operations, hurting companies' bottom lines, and can infringe upon the privacy and other human rights of consumers and the general public. Right now, there isn't much regulation around companies' cybersecurity practices. For example, Congress has not required that Internet of Things devices accept security updates, nor that consumer information be fully encrypted to limit the effects of a data breach. A Federal Communications Commission rule that would have required internet service providers to protect customers' information has been halted.

We did see some progress under the Obama administration. State governments are continuing the effort. And forward-thinking companies are beginning to apply concepts like active defense and corporate social responsibility to cyberspace. As cybersecurity regulations take shape, companies can choose to stay in the vanguard of progress – or simply react, following the rules as they develop.

Managers must think in new ways about data, communications, business law and even the ethics of trading off potential corporate benefits against risks to consumers' privacy. At stake is not only a firm's reputation but also, potentially, legal liability for failing to follow emerging industry standards. For example, Consumer Reports recently announced that it will be rating companies' cybersecurity and privacy practices. Businesses of all types, not just tech-centered ones, can help keep themselves in the clear by putting cybersecurity at the forefront of their risk management efforts.

A de facto standard of care

Although Congress has done relatively little about corporate cybersecurity standards, the U.S. government – in collaboration with industry – has created the National Institute for Standards and Technology Cybersecurity Framework. That document describes ways companies can evaluate their current networks' security and work to improve them.

The NIST Cybersecurity Framework is helping to define what constitutes a "standard of cybersecurity care" – a set of obligations companies owe to their customers, and increasingly their vendors and partners, as a basic practice of doing business.

Though the NIST Cybersecurity Framework was not published long ago – the first version came out in 2014 – and is technically voluntary, more consultants are telling companies to follow it. It is likely to be even more widely adopted if, as expected, it becomes a key part of an upcoming Trump administration cybersecurity executive order.

Standards like the NIST Cybersecurity Framework could become even more common not just across the U.S. but also internationally: Several dozen nations are rolling out their own similar guidelines.

Pressure from the feds

Under the Obama administration, the Federal Trade Commission pushed firms to improve their cybersecurity practices. In 2012, for example, the commission sued the Wyndham Hotel Group for storing data insecurely, enabling hackers to break in three times in two years and steal more than 600,000 credit card numbers and more than US$10 million.

As a result of the suit, the FTC ordered Wyndham to create a comprehensive cybersecurity policy, get it approved by independent analysts and update it regularly. That order is in effect for 20 years. The

ruling's power is still reverberating, in part because in 2015 it was upheld in federal court after Wyndham appealed.

It is too soon to tell how aggressive FTC cybersecurity and privacy enforcement actions will be under the Trump administration, though early signs are that they may ease somewhat.

States up the ante

Beyond federal action, some states are pushing forward, boosting consumers' privacy and security. California and New York are among the leaders, particularly in regulating data protections and requiring that customers be notified when breaches happen.

In 2016, for instance, California expanded its definition of the term "personal information" to include bank card information and PIN codes, as well as medical records and other identity data. California law also now not only requires that firms take measures to protect data themselves, but also demands strict safeguards when companies share customer information with third parties.

Similarly, New York issued a new regulation calling for companies to regularly audit and actively test security measures, and set up multi-factor authentication. Like the California law, New York's new rule could have broader effects because it applies not only to New York-based financial firms, but also to companies they do business with.

Moving from reaction to action

Companies will need to move away from reactive, defensive approaches to cybersecurity and toward more actively managing risk. That includes a range of technological and administrative shifts, some with financial

costs:

- Protecting administrative accounts and network routers with strong passwords, encryption, regular software updates and frequent checks to be sure no unauthorized devices or users connect to the network.
- Restricting remote access to systems such as by disabling file and printer sharing, as well as remote desktop controls when they're not needed.
- Scanning data storage for sensitive personal information, blocking or deleting any that is not actually necessary.
- Removing unneeded programs and files from computer storage, uninstalling and deleting them to prevent unauthorized access during a future attack.

But these policies are just the beginning. There is a push among cybersecurity professionals to go beyond existing formal requirements and get ahead of both attackers and regulators. This effort would seek not just to meet standards, but to exceed them. With ongoing, systemic cybersecurity risk management, companies can stay ahead of the curve, protecting their customers and society in the process.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation