Pooling Cyber Intelligence

cyber security risk management

Summary: Experts say there are ways that banks can share helpful information about cyber incidents, without divulging too much and violating privacy laws. We explain how this could work.

It seems German researchers find taller people are less likely than shorter people to get diabetes. We kid you not--for every 4 inch increase in height above the average, men have a 41% lower risk of diabetes and women have a 33% lower risk. Strange data point don't you think?

All day long bankers struggle to deal with other strange things, such as cyber threats. The good news is that more banks are sharing intelligence about them. But, there are still many banks whose board and management are nervous to tell others about what they've experienced. Many are also worried that sharing sensitive information could violate the USA PATRIOT Act or the EU's General Data Protection Regulation.

Experts say there are ways that banks can share enough about incidents without divulging proprietary practices or customers' personally identifiable information. Sharing the bad actor's methods and how a given bank might have handled it, can effectively inform others without endangering sensitive information.

One way to do this is to become a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry consortium with nearly 7,000 member financial institutions in more than 70 jurisdictions across the world. Banks can not only participate in peer-to-peer sharing of cyber threats, but information security officers (ISOs) can also receive threat intelligence reports - including summaries that the C-Suite and board members can understand, in addition to immediate phone calls when a cyber event is occurring.

Bank staff can also receive training through webinars and onsite meetings by the FS-ISAC on how to better detect and mitigate threats. There are even live events among members to game out best practices. One financial institution even said that participating in an FS-ISAC "war games exercise" to learn how to best defend a WannaCry-like ransomware attack was very beneficial; collaboration between members and analysts significantly improved everyone's response times.

Still another way to stay current on all of this is to attend cyber risk conferences or even local consortiums where you share intelligence with others. One banker depends upon what he calls "a circle of trust"--pooling intelligence not only with local financial institutions, but also with other local companies, as well as with clients and vendors.

In their latest data breach preparation study, Experian and the Ponemon Institute found that 51% of the ISOs surveyed say their organization shares or is planning to share cyber intelligence with government and industry peers. A significant majority (81%) say they benefit from the collaboration and incident response times have improved.

There are definite benefits to pooling cyber intelligence that not only protect your bank--but also your customers. As always, do your own research to see what works best for your bank's unique goals and needs.

<B>WEBINAR:</B> NEW EXPECTATIONS FOR Q FACTORS WITH CECL

Miss last months webinar on Q Factors? Join us for this second opportunity to learn about Q Factors. The Western Bankers Association hosts PCBB's Janet Leung as she talks about how Q Factors will vary based on the complexity of loan portfolio and chosen method. Also gain insights from the AICPA's guidelines for auditing CECL. Register