From the Sponsor EXECUTIVE FORUM **DATA SECURITY**

Cybersecurity and the TITANIC

On my office wall hangs a poster promoting the Titanic as the "world's largest liner." It is a lasting reminder that the biggest, newest, most expensive and modern technology can be foiled by a few relatively small mistakes. As Cybersecurity Awareness Month comes to a close, perhaps we can learn some lessons from the Titanic's Fate.

Don't be Complacent

Media hype at the time of Titanic's launching quoted the shipping line's owners as saying "God Himself could not sink her!" This expectation of invincibility affected the opinions and actions of passengers, crew and, indeed, the whole world, leading people to disbelieve the initial reports of the disaster. Rest assured that no information system is immune from a cyber attack. The right combination of threats, a lack of certain controls or inattentiveness can cause any network or business system to founder.

Don't Ignore the Warnings

Much has been made of Titanic's failure to slow down or stop, when all around her ships were doing just that while radioing Titanic of the threat they were seeing and experiencing. There is a robust community of cyber experts identifying and evaluating new cyber threats, and developing solutions that you can implement to reduce or eliminate your risk. The US Government, in the form of the National Institute of Standards and Technology (NIST), industry and trade groups and developers of firewalls and anti-malware software are all signaling threats and schemes and offering suggested responses, often tailored to your specific business or industry. You are not alone in cyberspace. Heed the warnings…they are real.

William Prohn
Managing Director
Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Keep looking forward

A mix-up in port before Titanic sailed meant that the lookouts in the "crow's nest" didn't have binoculars, which hindered their ability to spot the iceberg ahead. Keep an eye out to the future as your business grows and evolves. What new threats will you be subject to? How will working from home affect how you limit access to your sensitive data? How will the growth of on-line buying affect your selling and purchasing practices? How do you keep business and client credit card information secure?

Make sure your backup is sufficient

The protection of last resort, the "backup" of a liner at sea is her lifeboats. While no one would want to abandon ship for a small boat in the middle of the ocean, it's better than drowning! Everyone knows the Titanic didn't have enough lifeboats, even though they were compliant with regulations. Determine your data needs: what should be backed up, how long can you go without your system before a backup would need to be restored, where should your backed up data be stored, how frequently should you make a backup, etc. The "old rules" of copying to a tape once a month may no longer be adequate to protect you from today's threats like Ransomware. And, just like the lifeboat drills that are now required by all cruise liners (because of Titanic) test your backup periodically to see if you can actually restore the data!

Ask for help

Titanic's radio operators sent out one of the first S.O.S.'s in history, summoning dozens of ships (unfortunately too late) to her aid. If you are unsure of how a cyber attack could cripple your business or what controls might be effective (and cost-effective!) in your environment to protect your data, seek out professional guidance. You don't need to have a full-time staff of security professionals to implement a good cybersecurity program; and your own I.T. resources, good as they are, may not be current on cyber best practices. Also, not all the cyber threats are technical in nature. Look for the best way to regularly train and test your users in the safest on-line behaviors.

Don't become Infamous

More than 100 years later, the name Titanic is still a household word, and for all the wrong reasons. The monetary cost of a cyber event in the form of lost revenue, reconstruction costs or fines could prove insignificant compared to the reputational damage from the bad publicity and long memories of your customers and prospective customers. If you experience a breach, seek legal advice to determine what needs to be reported and who needs to be notified. While reporting requirements must be followed, you should seek to control the message and potential fallout from a breach.

User training and awareness, a risk analysis, effective controls, comprehensive plans to respond to an incident, a good backup and keeping your systems up-to-date with software patches can all help to keep your business afloat. Check out our STARTegy program to see how Dopkins & Company can help you with cybersecurity.