The Emerging and Evolving Threats of Cybercrime
Executive Summary

At the 27th Annual ACFE Global Fraud Conference in Las Vegas, June 12-17, 2016, the ACFE hosted an exclusive roundtable discussion for attending Corporate Alliance partners. Ryan Hubbs, CFE, CIA, CCEP, ACFE Faculty Member, moderated the event and focused the two-hour session around the latest organizational threats posed by cybercrime. According to Hubbs, fraud and cybercrime are beginning to merge, and with the singular growth of technology, more and more fraud cases will come with a cyber component. Below is a recap of the best practices and tools many of the Corporate Alliance partners in attendance are using to fight this global threat.

Evaluating the Risks of Cyberthreats

The risks associated with cyberthreats will unfortunately remain high as long as there are fallible users sitting behind a computer screen. “You are only as strong as your weakest link, and they [employees] are your weakest link,” said one partner.

In discussing how to best respond to these risks, the first best practice shared was to conduct phishing attacks on your employees to test vulnerabilities. If an employee fails the test by clicking on links and opening attachments, send him/her through additional training. Also consider tying bonuses and raises to the passing of tests.

Along with testing employees, the following suggestions were offered:

- Do not allow wire transfers to be authorized via email or fax.
- When there is a compromise, reach out to the bank that authorized the transaction as soon as possible to attempt to stop the transfer of funds. As one member suggested, “Tell them they are sitting on the proceeds of crime. You will find you get a much more respected and speedier response.”
- Use an attack or attempted attack as a case study to share with all employees. Consider using videos for training.
- For banks, educate your corporate clients about the risks of business email compromises.
- Educate your C-Suite and Board of Directors. Send regular cyberthreat updates to management. This helps reinforce the importance of not letting their guards down. Involve them in the role-play of an actual attack to show the true risk.
- Monitor executives’ accounts on LinkedIn and other social media platforms. If an executive does not have an account, imagine how easy it is for someone to create a fake account in his or her name.
- Use an existing disaster recovery plan as a model for how to react to a ransomware attack. The work has already been done and they share many similarities.
- Do not over-rely on cyber liability insurance coverage. It can contain loopholes and may not cover all risks.
Challenges to Executing an Effective Strategy

Some of the challenges in guarding against cyber risks mentioned by partners were budget restrictions, outdated legacy systems, the mobility of staff, balance of security and operations, time involved in implementing solutions and an inconsistent interpretation of policies (differing languages).

Among the solutions partners shared were:

- Remember that your contractors, suppliers and M&A targets pose a risk. Even if your organization has a strong security program, third parties could still be points-of-entry for cyberattacks.

- Instead of focusing on a budget for cybersecurity through one department like IT, try to package it in with all products or initiatives from other individual departments. One partner advised “When someone comes to you with a new product, say ‘Here are your risks, and you should budget for those.’”

- Conduct background checks and real-time activity monitoring on IT and cybersecurity personnel to help guard against insider threats.

Identifying Confidential and Proprietary Information

During the final roundtable discussion topic, partners shared the following ways they are dealing with risks involved with using the Cloud, personal mobile devices and third-party sharing sites:

- One partner mentioned keeping all files and data on internal servers and using one central hard drive. The company has even removed all CD drives and blocked USB ports for employees. When someone breaks the rules, they are written up.

- Implement guided processes for your employees to save and send emails. One company uses email automation rules to help employees save or send an email in three ways: internal, external or confidential. For example, if an email is being sent externally, it will say “Are you sure you want to do this?” In addition, an employee cannot send an email externally when it has been saved as confidential.

- Monitor employees to ensure they are not downloading anonymizing software. Also, remember to monitor third parties and contractors.

Conclusion

The threats posed by cybercrime will continue to evolve. And as technology grows, so will the need for organizational leaders to adapt and change their strategies. Anti-fraud professionals must partner with their cybersecurity teams in this ongoing fight. The sharing of best practices like those noted above will only increase the number of tools you have at your organization. As one partner mentioned during the conclusion of the session, “Don’t let this discussion stop today. The Corporate Alliance is an extra layer of trust for us when sharing best practices and information.”

To read more about what took place at the 27th Annual ACFE Global Fraud Conference, visit FraudConferenceNews.com.