Why Consulting Chemists Face Cyber Security Risks

According to the Commission on Theft of American Intellectual Property, international thieves steal around $300 billion of American intellectual property (IP) from U.S. companies annually. Cybercrime is now the most prevalent form of IP theft, and companies are justifiably concerned over every online interaction and device connected to their network.

The scientific community closely guards and values its IP as many companies rely on proprietary scientific information for their success. When hiring outside consultants, organizations expect contractors to adhere to the same standards of online behavior as every other employee.

When a contractor fails to uphold those standards and criminals infiltrate a company's network due to a consultant's negligence, litigation is an understandable response. Most consultants have access to an organization's firewall through login credentials, which can be harvested by phishing—even while working from a personal laptop. It's the consulting chemist's responsibility to understand cybercrime and the steps you can take to avoid being hacked.

What does cybercrime look like?

Most thieves use phishing or pretexting techniques to infiltrate a network, the former being the most popular of the two. Phishing is an email-based tactic. A cybercriminal sends what appears to be a legitimate email hoping an unwitting person opens an included attachment. One open attachment can install malware that allows hackers access to an organization's network.

In 2008, Chinese hackers targeted the aluminum company Alcoa by sending phishing emails to 19 senior employees claiming to be from Nissan CEO and Alcoa board member Carlos Ghosn. The email recipients believed they were opening an attached agenda for the upcoming board meeting and not malicious code.

All it took was a few people opening what appeared to be a legitimate email for cybercriminals to infiltrate Alcoa's network and steal almost 3,000 emails containing sensitive information.

Proceed with caution

Consulting chemists regularly handle IP and confidential client information inherent to the science industry. For that reason, always err on the side of caution when reading emails with suspicious attachments or hyperlinks, especially those coming from addresses you haven't received mail from in the past.

The 2019 Verizon Data Breach Incident Report implores people to think twice before opening an attachment or link that may be at all suspect in nature. You should send any communications that seem questionable to your client's IT department for review.

Another way to avoid a potential cyberattack is to remain up-to-date on all software and applications, even those not used for business purposes. Software updates often address bugs and security flaws that leave a computer or phone vulnerable to attack. To help avoid a potential hack, always accept software and operating system updates promptly or enable automatic updates to avoid disruption.

Even if you're cautious, there are unknown cyber risks, and one misstep could open you and your client up to criminals and bad actors. Cyber insurance—part of the Professional Liability plan for chemical consultants and available through Hays Companies—protects you from potential liability.

If you have any questions about cyber insurance or professional liability coverage available to ACS members, please contact Hays Companies at 888-437-7008.