ACUA Webinar
Ransomware – What's Next?
Q&A

1. How can non-IT staff contribute to keeping the organization safe (if it is even possible to use such a word)?

   A: Non-IT staff can play a major role in keeping an organization safe. Security is everyone's job not just IT and audit staff. Here are some ways to approach it.

   a) Make security awareness a 365 day campaign, but be creative so as not to develop cybersecurity fatigue. Rotate between units, buildings or schools, for example, a monthly cyber challenge or security related theme. Make it fun while building awareness.
   b) Develop an annual and mandatory security awareness training program for all staff (that includes executives), contractors, faculty and student-staff. There is affordable training software that is very good and can track completion.
   c) Develop a regular phishing campaign to reinforce training. Again, there is reasonability priced software that will do this. Remember, clicking on a link or attachment is the number one way ransomware and malware will enter your environment.
   d) No tailgating into areas requiring badge access and make sure badges are visible. Make it ok to say, "May I see your badge"? Be security minded.
   e) Insider threat unfortunately is very real. Establishes processes and policies for locking confidential material, ensure nothing is left on the workspace at night, etc. If I walked around the admin offices of your college or university tonight for example, what could I learn? How could I then use that information coupled with what is publicly available to hack your environment?
   f) Set screen saver policy to the shortest period your organization can tolerate. Many people leave their workstation without locking their screen. This invites trouble.

2. What laws require reporting cyber crime, and who do you report to and how?

   A: It depends. Your organization's Chief Information Security Officer (CISO) or others in senior leadership likely have established channels with local and federal law enforcement (FBI) to report and investigate various types of crimes, including cyber. If your campus has its own police department, they are likely the starting point. Where there is a data breach, each state has its own laws regarding notifying the data owner of the breach. For example, in California the law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined in the law, was acquired, or reasonably believed to have been acquired, by any unauthorized person. If the breach impacts 500 or more California residents the California Attorney General must be notified and other conditions apply.

3. If you have a policy of not paying the ransom, should you broadcast that as a deterrent?

   A: Definitely not. Criminals will not be deterred, and in fact could see it as a challenge to their skills and abilities. Game on!

4. I've heard that some cyber insurance carriers have been recommending always paying the ransom. Whether this is just so they can prove that cyber insurance is a good investments, does that mostly work? Or do a significant number of these situations still result in a loss of data?

A: There are many points-of-view on this topic and there is no right answer. KPMG as well as other organizations and the FBI recommends not paying the ransom. However, each organization and situation is unique. There are examples that once the ransom was paid the hacker did not provide the encryption key (surprise!) or the key they did provide did not work. There is also a concern that paying will invite the hacker back as the organization has demonstrated a willingness to pay. Remember, this is a crime of opportunity and if you pay, what stops the attacker from coming back again and again? The hacker just needs one vulnerability in your system or one user to click a link to return and make another ransom demand. Rather than investing in a strategy to pay, invest in the people and technology to harden your systems from attack.

5. Can you provide examples of "insufficient identity and access management"?

A: Identity access management is about enabling the right person to access the right resources at the right time for the right reasons. Not everyone needs access to everything all the time and using the framework of least privilege access is a good start. Here are a few examples of issues associated with insufficient identity and access management.

- If a change was made to a record of a critical application, do you know without effort who in your organization has read/write access to that application and when they last accessed the system?
- If management requested a list of everyone in the organization and what applications they had access to including admin privileges and they would like the list in 15 minutes, could you produce it?
- Do you know who as admin rights or is a "super" admin to each system and do you have policies and processes in place that govern the use of those rights?
- Do have separation of duties in both policy and practice for access?
- Do users with privilege accounts use them only when required or do they log in to the privilege account for all of their work.
- Are admin or user passwords shared? It happens all too frequently that admins for a specific application share a single password with other admins.
- Is there a policy in place to audit the use of privilege functions?

The best place to start is NIST 800-53 and the Access Controls family. Using that as your template you would be able to develop what "good" look like. There are many software products available today to automate these functions and give you a "single pane of glass" and governance for all IAM functions. At the very least, implement policies that govern access to critical assets.