Overview

6 Security Considerations for a Remote Workforce

Cory Ranschau, Manager of Information Security

Security teams have historically depended on the “castle-on-the-hill” approach when it comes to data security. All of their faculty and staff work devices were inside the castle walls, protected by moats and drawbridges. When new external security threats emerged — from new phishing tactics to malware vectors — they simply strengthened their walls or added alligators to their moats. But when the COVID-19 pandemic emerged, this approach was shattered while external threats simultaneously increased. Everyone moved outside the castle and lost the protective armor of the university network. With a growing remote workforce, the strategies listed below will help ensure faculty, staff and institutions remain protected.

1. **Protect your endpoint**
   Now that everyone is outside the castle walls, you must ensure your remote faculty and staff devices remain protected from viruses, malware and unauthorized access. Make sure you have an endpoint data protection solution in place and consider using cloud-deployed device management tools to make sweeping configuration changes across remote devices.

2. **Use a Virtual Private Network (VPN)**
   A VPN service will enable your remote workforce to establish secure online connections and communications between their home network and your institution's computer network. Require proper education on critical remote workforce tools like your VPN. You don’t want your faculty and staff using third-party VPNs. Have an official VPN that meets your institution’s needs and ensure that it is accessible and known to all faculty and staff.

3. **Secure identity and access management**
   Do you have good control over your user identities? This is especially important during workforce reductions or reorganizations. Make sure you are properly removing departing faculty and staff member’s access to your systems.
4. **Utilize cloud collaboration applications**
   Maintaining collaboration is essential for keeping remote workforces productive. Use tools like GoogleDocs and GoogleSheets, and set proper sharing permissions on important files so collaborators can edit and comment as needed. Consider making a shared drive where your team can store, search and access files from any device. This tip is especially important for HR leaders as they have become the new leading driver of the digital workforce experience largely based on these cloud applications.

5. **Personal use isn’t inherently ‘bad’**
   You need to be aware of the human element during situations or crises that require remote work. Faculty and staff make do with what they have at their disposal — using their work laptops to watch Netflix on their time off or taking Zoom calls with family and friends. Personal use will be more common, but this is not inherently bad as long as you reinforce security standards. Don’t bog your busy security teams down with babysitting personal use activity.

6. **Implement ongoing remote workforce training and education**
   Security teams should already have required training, but these are even more important during significant events that require remote work. Faculty and staff should be kept up-to-date on new and increasing security threats, especially when Google is finding 18 million COVID-19 related scam emails every day. Encourage your faculty and staff to have open and honest communication with your security team — ask them to flag any suspicious activity, and reinforce that they won’t be reprimanded for any security risks that they might accidentally trigger. This ongoing education, communication and awareness is crucial.

Remember to always consider your business’s unique needs, because every castle and kingdom is different and requires different protocols. We hope that these security tips will help your institution remain secure during crises that require remote workforces.