# Top Security Risks for SMEs in 2022

There are many articles that discuss the top and most common threats facing enterprises and organizations. All these attacks, threats, and risks are valid and will impact cybersecurity SMEs across the board. However, in this article, the goal is to set some of those threats aside and really look at what is impacting the individual behind the first line of defense for every organization. This is not to minimize ransomware, phishing, vulnerability, or patch management. These are all valid concerns that every organization should be addressing.

While the risks identified in this article are certainly at the individual SME level, these are risks that every organization should be considering and appropriately addressing. At some level, these impact the performance and capability of the organization’s security program and the overall well-being of its employees.

## Remote Work – Post Covid

Remote work was adopted as we all entered the COVID pandemic world. Many organizations placed years of work on their IT and security teams to enable their workforce to work remotely in order to accommodate local and federal requirements. In some cases, these solutions were deployed as a temporary fix or solution with no plans to do much else with them, as they would not be needed after COVID was under control. That has not been the case, as we see most companies returning to normal operations and embracing a highly distributed workforce like never before.

This adoption is great for the employees that want the flexibility but comes with challenges for the security and IT teams. In many cases, key controls and capabilities are still missing or have not been implemented. With these controls missing, it is creating more work, especially manual, for the security team to manage. This is adding to the burnout fuel for many organizations, which directly leads to issues with turnover and performance for the organization.

## Turnover

Turnover has been rampant across industries and across skill sets. This has been no different in security, but it is a trend that has been happening for many years, even before the great resignation. Turnover not only hurts team chemistry but also hurts morale for a myriad of reasons.

Turnover puts strain and additional work on every SME within a team. The required monitoring, daily tasks, and control maintenance need constant attention. In some teams, this can cause the team members that are still with the organization to need to take on additional work time. Couple this with the unknowns within the hiring process that can often be drawn out and result in a great deal of compromise on skill sets, and it only increases the stress on the organization and SMEs.

## User Awareness

It is a poor cliché that the weakest link of an organization’s security program are the people. While most individuals are well meaning and trying to find easier, more efficient ways to do their work, it can often create security holes or compromise points. Proper training and awareness campaigns are needed to make individuals aware as to why those pesky security controls are required and implemented. Some organizations are not investing near enough in this to assist the security team, as the value can be hard to conceptualize.

Investing in security awareness training, specifically phishing and social engineering, can help reduce the workload and security threats for the organization. Users are primary targets for many attacks, and phishing and social engineering continue to be a primary mode of deployment of malware, including ransomware. Additional training focused on good cyber hygiene is needed to make users aware of how to protect themselves and organization when conducting day to day work and engaging with online resources.

## Continued Training

Investment, not only cost, but more importantly time, to allow for continued training is sorely needed for SMEs. Security is not a stagnate industry, as threat actors have the advantage of being on the offensive side and being able to adjust their attack to take advantage of weakness in defensive controls. For this reason, it is critical for security SMEs to continue to upskill and train to understand technology advancements, changes in security controls, and industry best practices. It is unreasonable to expect a SME to be up to date and able to address the emerging security threats while working a full-time or over full-time job, without providing the time and investment for training.

It is critical for the organization to understand that the risk to a SME, while it is certainly the same as the organization risk, may not be in the same priority. Any SME in the security field would not want to be involved in a breach or ransomware event, but in most cases, they are not thinking about those day to day but rather the risks or lack of investment that is impacting them as an individual. The risks identified in this article are risks that many organizations have failed to think through or address, which is leading to more unsatisfied, stressed, and overworked security SMEs, which can lead to more exposure long term.