Security and the Unintended Consequences of Enhancements

We live in an age where innovation is king and staying still is not an option. There's ongoing pressure to develop new products or add new features to existing products on a continuous basis. Companies fear that if they don't have the shiniest object, someone else will lure their clients away with their shinier object. Much development focus goes to the shiny object side of products and services without quite so much intensity being applied to what happens when it gets let loose in the real world.

As these shiny enhancements are implemented in existing technology systems, this can create new security and privacy risks that need to be considered and mitigated. This can happen in the most unexpected places, ranging from Internet of Things (IoT) devices to core enterprise products.

At one law firm, expensive and bulky traditional snack vending machines were being replaced by a "trust but verify" system in which snacks were on shelves with an honor pay slot and a motion sensing IoT camera to investigate non-payment. Unless you picked up a snack, the camera did not come on or video record anyone, so the system seemed fine. But on review of the details of the program, it turned out that the cameras in each lunch room stayed on for 5 minutes with the least motion near the shelf and the cloud recording included sound which covered the entire lunch room for much of the time anyone was in the room. Putting random recordings of law firm lunch conversations into a relatively insecure cloud repository run by a food vendor did not seem like a good idea. However, it turned out that the microphones could be disable by unplugging them inside the IoT device, so the security and privacy goals could be met by an easy change to the hardware.

These cameras themselves have been seeing expansions in function. The basic recording security camera can also be purchased in the form of a doorbell, a portable Bluetooth music speaker and a car dashboard camera which monitors driving performance and location. Each of these expansions in functionality brings its own additional security and privacy concerns. On the privacy front, people make assumptions that the primary function of the device is the only function, which can lead to serious misunderstandings. The settings which control the privacy functions are not always stable, which can result in additional features being enabled through accident or software upgrades. On the security side, for devices which offer online storage, the data generally gets stored in shared cloud locations in these mass-produced devices. A typical past security design flaw of one model of cloud security camera recorded all the video for all owners of the camera with one Amazon cloud storage password. The consequence of that manufacturer shortcut, was that once a security researcher identified the cloud storage password on his device, he found he could access the videos of all the owners of the same model of device, which was certainly not the expectation of the other device owners.

These same problems are occurring at the other end of the enterprise software spectrum. Under pressure of the Covid-19 Pandemic, many organizations have expanded their use of collaboration technology to support remote work, including expanded use of Zoom and

Microsoft Teams. MS Teams was built on top of SharePoint Online and OneDrive, which is where documents and chats in MS Teams are stored. Building on top of existing Enterprise Technology let Microsoft create a competitive and useful system in record time.

But this approach has its problems as well. Many organizations, including law firms, have also been using SharePoint Online to create websites for clients. However, since MS Teams uses SharePoint Online for its own external user sharing, those SharePoint online settings carry over to the behavior of MS Teams sharing information. Each time a MS Teams team is created, an associated SharePoint Online site is created and the firm's global SharePoint Online external access settings will apply there as well. This conflict between the SharePoint external sharing settings a firm wants for its' client SharePoint sites and the external access settings it wants for the SharePoint Online sites created for each client MS Teams team are generally not the same. This conflict has been sufficiently problematic that some firms have gone so far as to use a different O365 domain for the two functions.

Microsoft has been steadily improving the situation with additional governance controls and monitoring, especially for organizations which have licensed E5. But firms we work with are not finding the problems are fully resolved. Like other SaS vendors, Microsoft has been rolling these new features and controls out through automatic upgrades which puts more pressure on law firms to identify the new problems created by each new automatic MS Teams and SharePoint Online update.

In the past, IT departments had the luxury of receiving updates, evaluating them on a test system and determining if and when they might make their way into the live system. With the proliferation of cloud services, updates are being applied at software vendor rather than client convenience. Most medium and large law firms have a change management process designed to look at the privacy and cyber security risks associated with firm-initiated changes, but many firms are struggling to adopt their change management process to regular feature upgrades pushed by Microsoft and their other cloud vendors. Firms need to stay ahead of Microsoft and other cloud vendor upgrade plans so that security settings are adjusted to conform to security and governance policies.

IT departments used to spend a significant amount of their time planning for and evaluating upgrades to core systems. Much of this upgrade effort has now been removed in a SaaS environment. The overall effort, though, may not have diminished as much as vendors would like to have you believe because firms now need to apply their focus to the understanding of pending changes and how those changes, both functional and those related to security, impact their own unique environment. This requires a slightly different mindset. It is no longer possible to test and observe what happens when an upgrade is applied. An IT department has to understand their environment intimately, analyze the changes that a vendor is due to release and evaluate the impact. Constant vigilance will be the only way to avoid the unintended consequences of the shiny new objects.