Cybersecurity and Door Handles

What is "cybersecurity?" Cybersecurity is simply protecting anything electronic that is networked, typically through the Internet. This means computers and other devices, and the data that is stored on them. It also means protecting these systems from outside hackers and internal errors. What do door handles have to do with it? Door handles have a lot to do with cybersecurity, at least with helping to understand some of the major threats and responses faced by businesses today.

The most common response to the topic of cybersecurity or information security is "Who would want to hack our systems? We don't have anything that anyone would want!" While it is true that government agencies, large companies or critical infrastructure might be targeted by foreign agents or other hackers, most infiltrations are the result of random (but systematized) attacks. Fairly regularly, there are reports of cars being broken into by gangs of kids wandering the streets at night. The police urge residents to be sure to lock their cars and remove valuables. The scenario is a group of hooligans walking down the middle of the street, pulling on car door handles. If the car is locked, they walk on. If the door opens, they take advantage of the opportunity to rifle through the car, glovebox, trunk, etc. The attack is a random, but systematized try on a series of targets, without regard to the potential value of the target.

William M. Prohn
Managing Director,
Dopkins & Company, LLP

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Once the door is opened, there are additional steps that could help protect the car's contents, such as an alarm which sounds when the door opens; valuables secured behind additional door handles in the glovebox or trunk, which are separately locked; and comprehensive auto insurance to help pay for any loss. Keeping the car in a locked garage (another door handle!) could offer an even greater protection of the vehicle and its contents.

A typical cyber threat is an automated attempt to log in to every public IP address found on the Internet. If the login attempt is unsuccessful, the attack moves on to the next IP address. If the login attempt succeeds, either because there are weak passwords, or a poorly configured firewall, the hackers proceed to rifle the virtual glovebox and trunk of the network, looking for valuables. The common ways to protect against this attack offer lessons for cybersecurity.

First, keep the car door locked. While the windows (no pun intended) could still be broken, or the tires slashed, in general there are plenty more easy targets just down the road. Strong passwords regularly changed and properly configured firewalls provide this type of barrier like a locked door handle. A series of automated log in attempts will fail to gain access, and the threat will move on. A well configured firewall with various layers of prevention and detection can stop the intruder and, like an alarm system, alert the user to the nature of the attack to allow for a more specific response.

If an intrusion does take place, damage can be mitigated by having identified the most sensitive systems and information and segregating these with additional permissions and passwords. These access controls (or internal door handles) not only represent further barriers to an outside hacker, but also help to prevent malicious or mistaken activity by legitimate users and employees, by blocking their ability to reach systems which are not part of their duties.

Cyber liability insurance, like comprehensive auto and theft protection, can help mitigate the loss if an attack is successful, assuming your coverages and deductibles are appropriate. This requires a clear understanding of the value of the assets and risks faced, which is easier when it comes to cars than cyber assets. An I.T. Risk Assessment will help identify the risks and define the value of systems and information in a way typically not needed when buying car insurance. Similarly, parking your systems in a more secure place, like a well-managed cloud provider, can offer additional levels of protection, just like parking your car in a garage.

A typical cyber threat is an attempt to log in to every IP address found on the Internet. If the login attempt succeeds, the hackers proceed to rifle the virtual glovebox, looking for valuables.

A final lesson from door handles is one that we all commonly do when locking a door: jiggle the door handle. It's almost an unconscious reflex to make sure that the door really is locked. This additional assurance (an audit) verifies that what we thought we did was actually done. Any number of locks or door handles provide no security if they aren't locked. Leaving the door open just one time can mean the difference, when the random, systematized threat comes along. A regimen of periodic auditing of the key controls in place to verify that they are effective and working properly, is a necessary on-going step, after all the other controls and door handles are in place.