Identify What's Missing from Our Cyber-Security Posture

Ignoring cyber-security risks and avoiding protective steps could put your franchise system in peril.

BY BRUCE SCHAEFFER AND HENRY CHAN

In May 2014, a former multiple-unit Subway franchisee pleaded guilty to a scheme involving gift cards and tampering with Subway's computerized cash registers. Shahin Abdollahi, 46, of Lake Elsinore, Calif., sold point-of-sale systems to at least 13 other Subway units on which he had secretly installed remote software called LogMeIn.

When the stores were closed, he and his co-defendant accessed the systems and loaded up to $40,000 in value onto Subway gift cards which the two men then sold on eBay and Craigslist.

But that was just small time stuff. More recently there have been big hack jobs at Target, JP Morgan and many other businesses causing extensive damage in the millions of dollars. Then there was the hack at Sony, where many management people at the top lost their jobs. This particular hack involved spear phishing attacks — the use of everyday email injected with malware installed into a computer system when an unknowing user clicks on a link — to gain entry into their network.

The general description of the culprit in all these instances is "destructive malware," a form of corruption which has been around almost four decades. But its recent appearance in many new disguises inside enterprise networks has shone the light on the enormous destructive capabilities of such worms and viruses.

PLANNING THE RESPONSE TO A DESTRUCTIVE MALWARE ATTACK

Dealing with a DM incident is too important to just leave to the IT professionals. Bringing in expert cyber-security professionals is the only answer and even that is not perfect. Remember, mega-credit card processor Heartland Payment Systems was hacked despite being fully compliant with the security controls mandated by the Payment Card Industry Data Security Standards the day before it was compromised.

The job of protection is never-ending. As is carved into the cornerstone of the U.S. Capitol, "The price of freedom is eternal vigilance." Resting on some anti-virus or malware protection is only as good as the last discovered hacker. New forms of DM are concocted every day by very smart people whose only job is to cause your business trouble and steal from it. They work all day every day all over the world (e.g., North Korea, Iran, Ukraine, Belarus, Russia, etc.) to do harm to the systems of others. And there are the home-grown hackers too.

The geography of exposure is not limited just to the franchisor and its franchisees; cyber-security must address all the system's business relationships and partners. If any of those third parties with access to the franchisor's system suffer DM attacks, the franchisor had better assess all their connections too, to assure there is no possible cascading impact to the franchise system, and to make certain that the franchisor's information security technology is capable of defending against that particular threat. Significant incidents at related firms or business partners should always serve as a wake-up call for a franchise system to conduct additional cyber-security risk assessments and test its crisis action plans.

BEST PRACTICES: THE FIRST STEP – MALWARE DETECTION

As soon as any DM is detected in a franchise system or in the system of any vendor, partner or other business relationship, it is of the utmost importance to see if the same or similar DM is lying in wait in its own system. In the Sony hack, for example, its security vendors such as Kaspersky, Symantec and Trend Micro were the first to advise them of "indicators of compromise" connected to the DM.

If this happens in your franchise system, your cyber-security team and other network defenders must compile all IOCs (and continue searching for more) to find out if the franchise system's current anti-virus and malware providers are detecting and blocking this particular DM.

BEST PRACTICES: THE SECOND STEP – VULNERABILITY ASSESSMENT TESTING

If your system is a victim, the next step is to conduct extensive testing. If your system has not yet been a victim, the same VA testing should be done on a prophylactic basis:

1. Stolen user names and passwords: What is your policy for authentication to prevent the use of stolen IDs?
2. Employee entitlement changes: What happens in your system if DM compromises an administrator account? Is your system prepared to react to that?
3. Disabling processes: If DM disables critical processes how will you know? Will your system generate an alert?
4. Compromised Anti-Virus: If the DM is new or takes steps to disable your system's AV will you get an alert? What will you do then?
5. Exfiltration: If the DM is exfiltrating critical data how will you detect it? Once detected what will you do to stop it?
6. System restoration: Do you have a plan? Is it memorialized only on the same computer systems that have been compromised? That's not a good idea.

BEST PRACTICES: THE THIRD STEP – RECOVERY PLANNING

In the report "Contingency Planning Guide for Federal Information Systems: Detection and Analysis, Containment, Eradication, Recovery and Post-Incident Activity," the National Institute of Standards and Technology describes the basic elements that go into a response to a DM incident. To minimize the impact and financial losses from system downtime caused by DM any prepared franchise system must establish and/or update at least the following on a regular basis:

1. Crisis Management Plan: If there is a DM event, every business asset perceived as vital i.e., websites, customer lists, personnel and payroll records must undergo a thorough business impact assessment (preferably prior to a crisis event).
2. Disaster Recovery Plans: A DM incident can quickly become a full-blown crisis event for a franchise system (or any other business) if critical business computer systems fail and restoration cannot be completed quickly enough. Any sound disaster recovery plan should provide for the company's critical applications and network connectivity to be moved to a back-up site until the system's main units can be cleared of the malware.
3. Enterprise Level Backups: A company must have a well-documented and tested back up plan to be put into effect if it is compromised by DM. Whether via tape, disk or cloud type services, a comprehensive document that establishes backup procedures and contact information is an absolute necessity for reconstituting networks and systems.
4. Hard Copy Resources: Any of the following can be stored on a franchisor's computer system but hard copy must be readily available in the event computer networks and systems are put out of action:
   - Inventory of all critical systems and applications; contact information for all essential personnel.
   - Secure communications procedures for recovery teams; contact information for external resources.
   - Service contract numbers to get vendor support; licensing/activation keys for operating systems.
   - System and application documentation; system and application configuration backup files.
   - Data backup files; system and application integrity tests and acceptance checklists.

Destructive malware is a world-wide threat both to domestic and particularly to international franchisors. Management that ignores the risks inherent in cyber-security and downplays the need for insurance and professional advice and continuing penetration testing does so at its own peril and is beyond irresponsible. ■

Henry Chan, a computer and network technology expert is a co-founder of Franchise Technology Risk Management providing cybersecurity services to the franchise community. Bruce Schaeffer is an attorney and franchise valuations expert based in New York City. Find them at fransocial.franchise.org.