The Road Back: Recovery from a Malware Attack in the Long Term

Arete Incident Response is currently answering the call of duty for about 60 companies per month who have experienced malware intrusions. These are mostly ransomware or business email compromise attacks. Arete's primary goal is to restore what was broken and get the client back into business. However, another important goal is to harden the client's IT environment against future attacks.

The steps taken by Arete commonly involve the following:

- Implementing a more secure login process, such as two factor authentication—especially for remote access
- Installing endpoint protection agents, which some call "Next Gen AV", but are far more than just antivirus software
- Minimizing the attack service by disabling unneeded services and protocols; and
- Changing passwords, particularly on administrative accounts.

During the initial stages of the response process, the Arete team is completely focused on remediating the malware and getting the client's critical systems back online. But what does this experience mean for the future of the company? Usually, the business owner has some regret about not having taken sufficient security precautions before the incident, and the question always arises: "How do we keep this from happening again?"

One critical piece has already been implemented – endpoint protection. Comprehensive coverage of the network boundaries increases the chances that intrusions will be detected. However, cyber-extortion/ransomware and the malware that enables it can evolve rapidly and require a continuously trained staff to thwart. Acquiring, retaining, and training adequate staff is beyond the capability of many businesses. A cybersecurity firm offering vCISO (virtual chief security officer) services can provide the needed expertise to ensure that the business develops a formal information security program that addresses current risk, as well as prepares for the next wave of attacks.

Preventing the recurrence of a breach involves more than technology and requires a more comprehensive approach to security. Information security is not just a technical problem–it is a business problem. It should be approached in the same methodical fashion by which other business problems are managed. Just as the company has a "quality culture" for products, it must be understood that security is just another aspect of product and service quality. Quality is achieved through deliberate and continuous actions. The development of policies, standards of behavior, and contingency protocols for security should run parallel to the critical business processes that generate revenue. A successful security program requires some investment, but in the long run pays off in safeguarding the business' data, intellectual property, consumer information, business processes and most importantly, its reputation.

A comprehensive treatment of a full security program is beyond the scope of this article. Nevertheless, significant components include:

- IT policy that clearly establishes expectations that management has regarding the protection and handling of company/customer data, company technology and resources.
- IT infrastructure review for assessing the current

state of company technology and means of access to that technology, with a roadmap of continuous security improvement.

- Data security and privacy reviews that map the movement and protection of sensitive data as that data traverses the critical business activities and processes.
- Special attention should be paid to understanding what is most important to continue generating revenue, with contingency planning for disaster recovery and business resilience for each critical process. The people, processes and technology that actually make the business what it is should be well understood, documented, and have redundant resources for ensuring continuous operations, even during a cyber-attack.

Spending on improving the security posture of a business can be a hard pill to swallow, particularly after expenses from a breach come in, but there will never be a better moment to tackle it. Security events can be a focal point for employee awareness, and the need to heighten that awareness will never make more sense than in the days following the event. Building a culture of security and framing the effort required as just another part of the business day is a relatively low-cost way to improve. Other investments in maturing processes and technology will probably be required to ensure a secure future for the business. The best way to spend on security could be to acquire the services of those who have built programs before, at least until there is a functioning security program that can stand on its own two feet.