



**LAYERED
DEFENSE**

Why Businesses Today Need A **LAYERED DEFENSE**



By Milton Bartley, *ImageQuest founder*, and
Brad Lyttle, *Vice President of Information Technology*

Remember the good old days when you could buy an anti-virus software CD, install it, and your systems and data were adequately secured?

Sadly those days are long gone. Today small and medium businesses face cyber threats that have grown increasingly sophisticated, targeted, and persistent. Your small business is an ongoing target for hackers working for hostile foreign countries. The target on your back is even bigger if you are a regulated company or one doing business with regulated companies.

Like it or not, your company holds - or has access to - data that these hostile hackers want.

"Your small business is a target for hackers. The target on your back is even larger if you do business with a regulated organization."



Single-focus controls such as a firewall or anti-virus are only a starting point to protecting your critical networks and data.

They are using bots, Social Media research, impersonation, and monitoring to figure out how to crack open your network. An attack that results in data loss can be devastating – with long-term financial and reputational effects.

While your simple anti-virus software and other well-designed single-focus controls (e.g., firewall and spam filters) worked well in the past to stop specific attacks, the bad guys' advanced capabilities are now so sophisticated that single-layer protections inevitably fail.

Reliable studies will tell you that 97% of reported incidents were easily avoidable. The affected organizations became breach victims because they believed the misconception that having a firewall and anti-virus software installed at their facility and on their computers was enough. The truth is these measures are only a starting point in protecting your critical networks and data.

CUT CORNERS TO SAVE MONEY – AND SPEND MORE WHEN YOU'RE HACKED

ImageQuest takes a cybersecurity-first approach. That means we put your network and data security ahead of other considerations when we design, upgrade, and provide ongoing support to your systems. When you invest in ImageQuest, you are paying us to prevent and mitigate IT problems – including being hacked.

We employ multiple security controls in a layered approach that ensures a gap or a weakness in a single control won't necessarily lead to an exploit by the bad guys. This layered security approach is the most effective way to shield your network and data from today's most sophisticated threats.

You probably take a similar approach to secure your home and your family. You have locks on your doors, a security alarm, and possibly security cameras. A burglar may overcome one or even two of these controls, but with each layer you add, the likelihood the burglar is discouraged and leaves to seek easier targets increases markedly.

In the same way, ImageQuest's layered security approach provides interlocking security controls to help our clients avoid attacks from multiple potential vectors. Those vectors can include phishing and spear-phishing (phishing targeted at a specific individual or organization), brute-force attacks, denial-of-service attacks, malware, or code injection.

The vendor who is offering you discounted security solutions will recoup those savings the minute you start having issues. And we guarantee the discounters will leave you with issues. With us, you pay to AVOID problems.

YOUR BUSINESS IS YOUR CASTLE – DEFEND IT!

Layered Defense is not a new concept. Castles also employed layers of defenses. See if you think some goals sound familiar.

CURTAIN WALL – Built several feet thick, with huge rocks. Designed to withstand battering rams and projectiles.

TOWER – The first detection and response. Typically taller than the walls to provide a better view of oncoming attackers. The stairs inside towers turned clockwise, making it harder for right-handed attackers to fight. Defenders had more room to swing their weapon hands.

DRAWBRIDGE – The original firewall. These raised up or swiveled to break the pathway to the castle.

MOAT – Water around a castle protected it from attackers tunneling under the castle. Attackers entering the water would drown. Some moats also hid sharpened stakes for attackers who persisted in wading in.

BARBICAN – Perhaps the original multi-factor authentication. Added in front of gatehouses with an extra gate, narrow twisty pathways that gave defenders a good view of – and good aim at – entrants.

GATEHOUSE – These had iron or wooden gates that could be shut to halt attackers. Some gatehouses also had holes through which defenders poured hot liquids and dropped rocks to discourage attackers. Archers also used slits to shoot at attackers.

BAILEY – An inner courtyard. If attackers made it this far, they were exposed to archers shooting from crenelated protection. 🏰



WHAT LAYERS DO YOU NEED?

Each attempted attack can be different, and there is no magic bullet to combat them all. Hence, we use the sound defense strategy of **Prevention, Detection, and Response**.

PREVENTION is the broadest category and includes the protections you're familiar with: firewalls, anti-virus software, spam filtering.

Employee Security Awareness Training. This is one of the most successful ways to prevent cyber attacks. FBI cyber experts agree that an effective Security Awareness program, as part of a layered security approach, can be as much as 95% successful in preventing today's sophisticated attacks.

For that reason, ImageQuest strongly recommends our clients incorporate Security Awareness training into their cybersecurity programs. Your systems today require a professional approach from your employees – down to HR policies that dictate access practices and other use policies.

Personal Device and Home Network Security. While we're on the topic of your team, you also have to think about how they are accessing your system. Increasingly, that is on personal devices – tablets, smartphones - and from home networks. Since you don't know what bugs or malware those devices have acquired during personal use, you must think about security protection here as well.

Consistent, prompt, security patching program. We insist on this. Many of the more notorious security breaches in recent history were a direct result of organizations not employing a consistent security patching strategy. The WannaCry Ransomware attack in May 2017 that affected global companies the likes of Maersk, DLA Piper, and FedEx targeted organizations running the Microsoft Windows operating system that had not applied a recent security patch. Similarly, the Equifax breach later that same year was directly tied to the Equifax IT team failing to update critical servers with a known security patch.

Thus, a security program architected by ImageQuest always includes a consistent patching strategy.

DETECTION is another critical aspect of cybersecurity that, unfortunately, some organizations neglect.

This can include **Multi-Factor Authentication, IP or geographic access restrictions, account lockout for too many attempted log-ins.**

Detection mechanisms can also alert either the affected individual, the organization's IT Security team or both to potential fraudulent access.

Detection also allows ImageQuest security experts to analyze incidents and determine which security controls are working and which may need to be tweaked or augmented.

Managed Detection and Response. Some clients need this level for continuous network monitoring for anomalies that may indicate the start of an intrusion or attack. At this level, ImageQuest provides a 24/7 Security Operations Center (SOC) that uses artificial intelligence combined with human Security Engineers to let us know proactively if something is amiss.

RESPONSE is another broad category that encompasses both the speed with which an organization reacts to a potential incident to how they use that data to improve their security posture. Time is money, and reaction time in the face of a possible security incident is no exception. The faster your security team can respond, the more likely they can minimize any potential negative impact.

SOC-as-a-Service. We offer access to a SOC for clients who need one but cannot build their own. The SOC can give us a critical head start in stopping intrusions and attacks. We work with a service that is continuously monitoring attacks across the globe and has the expertise to spot deployments of new, evolving malware.

Incident Documentation. A less obvious response tactic is applying lessons-learned to tweak and improve your overall security posture. That starts with clearly documenting every incident regardless of the outcome and impact. ImageQuest helps clients implement a consistent process that serves to satisfy regulators while providing steady security improvements.

Incident Response Exercises. We help you think through how various decisions and actions will impact your organization and your critical stakeholders in a real situation. We follow the practice of first responders – rehearsing or testing your organization's response to a security incident. We review your policies, conduct relevant scanning and testing, and discuss the results with you.

Testing processes and procedures before there is an actual incident can help validate the effectiveness of your various security layers. Just as importantly, training with real-world scenarios increases the likelihood that your employees will react with appropriate speed and efficacy if there is an actual incident.

ImageQuest's Incident Response exercises are a critical piece of any well-designed cybersecurity strategy.

CONCLUSION

In today's environment, you must deploy a layered approach to cybersecurity that effectively shrinks your organization's vulnerabilities to determined hackers. The consequences of a successful attack are just too risky to leave your defense to an outdated strategy.

If you want to learn more about how our layered security approach would help your organization, contact ImageQuest today! 

