Reducing the Likelihood of Computer Compromise

A Small to Medium Business Guide

By Ken Foster, KMBL Security
January 7, 2012

Virtually every business and organization today uses some sort of information technology in their daily operations. The gambit ranges from a small business using a spreadsheet for a ledger, to a large multinational corporation using a complex online presence with shopping services and everything in between. Regardless of your size and IT support team, every organization must take steps to ensure their data is protected from compromise, theft, or loss. Use the following the guidelines to lower your overall risks:

The first thing to understand is securing your information takes some effort. The amount of effort you exert should be proportionate to the value of the information. For instance, if you run a business that has gross sales of $100,000 a year, you would not spend $20,000 on network security solutions. However, it's not unreasonable to consider a capital outlay in the neighborhood of $2,000 for the same business. Ultimately, your investments in information security are designed to protect your business operations. Think of information security like you would an alarm system on your office or liability insurance; it's a risk mitigation step designed to allow your business to remain viable. Areas you must consider are broken down into the following seven basic areas:

- Basic Network Perimeter Security
- Individual Client Security
- Physical Security
- Logical Security
- Data Classification
- Data Preservation
- User Education

Basic Network Perimeter Security: Far too many people assume they are too small or insignificant for a cyber-criminal to be interested in their information. This is the wrong attitude, often leading to intrusion, customer data exfiltration, and irreversible damage to client confidence. Today, anyone with a broadband network connection (including your home computer) has value to a cyber-criminal. Begin your evaluation with how you protect your network connection. Perform a physical review of your service, from the location it enters your facility to the time it connects to your computer. For simple installations, there may only be a cable modem or DSL router between your computer and the provider. In larger network operations, this complexity increases with the introduction of firewalls, routers,

Intrusion Detection (IDS) taps, and Layer-3 switches. Regardless of how complex ask yourself the following questions:

- Is there a Hardware Firewall between my network and the provider? If not, that is where you *must* start. Even a mom and pop business should have a basic hardware firewall. This isn't the one that was included inside your Linksys or Netgear Router, but a real firewall. Use that firewall to prevent dangerous traffic from getting to your computers and monitor outbound traffic from your network for signs an uninvited guest may already be there. There are several companies that make excellent small to medium-sized business solutions. Do your own research but consider companies like Astaro and the UTM Series from Netgear. It doesn't cost very much for a simple to implement solution. You would be surprised how much a few hundred dollars will buy today!
- Do any of your computers have Dial-up Modems installed? Depending on the age and requirements, you may still have desktop computers with modems. Almost every laptop still operating today has a modem as well. If you allow a computer with a modem to be connected to your network and a telephone line at the same time, you effectively bridge (by-pass) all your External Network Security efforts. It's almost unheard of today for a legitimate need for a modem in a desktop system. Remove them if possible; at a minimum disable them in the control panel. For laptops, disable them in the control panel (as they are integrated to the system motherboard and non-removable). Since most internet service providers' no longer routinely provide modem access to their networks, consider these a security risk.
- Do you use WIFI Wireless networks? Significant advances have been made by hackers with regard to tools used to capture and brute force attack wireless passwords. If you can at all afford to avoid using wireless, do it. If you can't, they consider using a combination of a Demilitarized Zone (DMZ) on your firewall and Media Access Control address (MAC address) filtering to connect your Wireless router. While MAC Filtering is not infallible, its better than nothing.
- Do you use Cellular Wireless networks? These can be either through your smartphone hotspot or by using a USB Aircard. If you do, make sure you are not allowing your systems to be connected to more than one network at a time; see bridging above.

Individual Client Security: Even though you have spent time and effort ensuring the exterior of your network is secure, that doesn't mean you are done. Sometimes despite your best efforts, a bad guy gets inside your network. This can occur because of malware delivered via email, compromised webpages visited, or zero-day exploits. Depending on your chosen solution, some of these risks can be reduced or eliminated at the firewall. However, no solution is 100% perfect every time. You need to protect your computers inside your network.

- Client Protection Suites: Every computer should have software installed that provides for a software-based firewall and Anti-virus / malware protection. There are several large providers in the market space. If you have more than ten computers to protect, consider a centralized

management solution. It is just as critical you attempt to prevent the infection as it is to know when one occurs.

- Firewall Services: Now you may think, why do you need a hardware and software firewall? This is because if compromising traffic makes it through your hardware firewall, you have a second (layered) defense using the software firewall. You can also use the software firewall to restrict access to resources and applications. As an example, the owner might need network access to the payroll clerks' computer, but you do not want regular employees accessing this data. This can be accomplished easily using this method.
- Anti-Virus / Malware Services: This pretty much goes without saying that in today's computer world, this is a must have item. Do be fooled into thinking if you use Macintosh or Linux you are immune. Many exploits today leverage blended attacks that use widely available software such as Adobe Acrobat Reader and Flash; these are present on most computers regardless of operating system. Don't forget to check to see if you still are receiving current signature updates from your AV solution provider. You would be surprised how many people have expired maintenance on their AV solutions and are not. When it comes to picking an AV provider, this is where personal preference and comfort come into play. Pick a package that meets your needs and comfort level. If you are tracking many systems, consider purchasing a hosted or managed solution. It's as important to know what you stopped as what got through. When a system is infected and later discovered as the result of scheduled scan, you can no longer trust the integrity of the system. Simply using a removal tool to clean the infection doesn't mean the system is secure. As painful as it is, you should use the manufacture reinstall disks are restore the system back to its last known-good baseline. Anything less, risks reintroduction of the malware into the system and others later. This is why data preservation is so critical and covered later in this paper.
- Host-Based Intrusion Prevention Services: Some client suites provide in addition to firewall services, a local monitor to detect unusual behavior-based actions. Referred to as Host-based Intrusion Detection / Prevention, this software attempts to halt malware actions. This type of software is particularly useful against unknown and zero-day exploits. If these options are available in your client suite, this is an excellent addition to your protective posture. This software requires some training, so be prepared to spend a little time approving actions after its initial install.

Physical Security: This is an obvious area that is far too often overlooked. If you give me 30 minutes of uninterrupted quality time with anyone physical machine, I can do very nasty things to it. This holds true for all information systems. If you have servers, they should be in a locked room. Use card log access control if possible, at a minimum a deadbolt lock. If that is not possible, then a locked cabinet (both doors) with limited key access is a good fallback position. If this level of control is not possible, at a minimum attempt to dissuade unauthorized access through the use of video monitoring or other

methods. If someone ever does obtain unauthorized access to a system, you must assume the system is compromised; reimaging to your baseline and restoring data is the only safe recovery method. Never reconnect a potentially compromised system to your network. Someone else may have control of the system, providing them a backdoor to your network for later use.

Logical Security: This concept follows the generalized rule of Principal of Least Privilege. In the days of Windows XP, everyone who had a logon to the computer was a full blown Administrator. This is why there were so many compromised systems during XP heydays. The best method to implement logical security is through the use of a unified Directory Service (e.g. Active Directory). This provides users with a managed logon credential for all resources on the network. If you can't implement a Directory Service, these next steps become harder to implement. Use the guidelines below to establish some barriers to compromise:

- Roles and Responsibilities: Make a list of different roles within your organization. An example of a role might include shipping, payroll, human resources, etc… Next determine who are responsible to fill those roles. If possible, divide roles in between knowledge workers and managers for better access control. Be sure to understand any applicable regulatory requirements that apply to your business; they may require further granular roles for administrative controls as well.
- Separate Administrator and User Level Account Access: Simply put, never allow someone with privileged level access to a system (e.g. System Administrator) to use their standard level user account to perform those functions. This is for two very real reasons. First, external compromise from email or malicious websites is most likely to occur on their normal user account. If their normal user account is compromised, they only have access to their system and what systems their normal user role allows. However, if they compromise your administrator account, you have handed them the keys to the kingdom. Never allow a Privledged User Account to be used for email or causal internet use. Secondly, acceptable resource access is easier to log and audit if you separate the roles. Consider a Network Administrator a role and act accordingly.
- Create Access Control Lists (ACLs) appropriate to established roles: As we covered in Roles and Responsibilities above, you should limit access to files, data, and other resources based on the least amount of access an employee needs to accomplish their job. This is called the Principal of Least Privilege. This prevents employees from accessing data outside of their job description. As an example, it is not reasonable for the sales team to be access the payroll records of their manager or other co-workers. ACL's should be granted so that access to resources by workers can't be accidently or maliciously modified. For example, the sales catalog might be accessed by the entire sales team. Only the Manager should be able to update the catalog. In this scenario, the sales team might be in the Sales Read Only role which enforces list and read access to that directory, while the Sales Manager might be in the Sales Full Access role, with create and modify permissions. ACLs can be complicated to implement so understanding the implications of your

decisions are critical. For additional research consider the PCGuide reference of this material as a starter.

- Encrypt Critical Information: Data that you classify as sensitive (covered below) should be encrypted. You do not need expensive hardware or software to accomplish this task. Consider using utilities already available in your operating system or a 3rd party freeware solution such as Trucrypt to perform this task. Encryption provides two critical functions:
    - Limits Unauthorized Access: By encrypting your data, anyone without appropriate access is unable to casually view, modify, or share the data. Encrypted data without the decryption key appears to that user as incomprehensible gibberish.
    - Limits Liability: Encrypting your data, lowers the risk of data compromise. This provides you and your clients a level of assurance that this information is accessed inappropriately, it can't be used. Depending on the type of data, some regulatory guidelines may require data encryption, always check your requirements.

Data Classification: This is the concept of identifying which data is of a higher value others and providing an appropriate level of protection based on that label. For instance most businesses have public data. This is data you intend to be widely shared as part of your business model. This data requires the lowest level of protection; prevent modification as an example. However there are other levels of data that you may consider far more critical to the viability of your business, requiring more effort to protect. Here are some example classifications to consider:

- Public – Press Releases, Web site information, Sales Flyers and handouts, etc…
- Sensitive – Future product releases, Internal working memorandums or directives, daily operations information, costs, current supplier contracts, etc…
- R&D – Research about products in development, competitive product analysis, documents pertaining to future markets, design plans, etc…
- HR – Any data related to the personnel status, pay, or employment records of current or past employees, Non-disclosure agreements, etc...

Once you have determined the level of classification, you can assess a cost to the organization if this data were to be released to the public, a competitor, or destroyed. There are several excellent tools you can use to perform this risk analysis. For a primer on data classification, please see Tom Bower's article on How to conduct a data classification assessment.

Data Preservation: Now that you have secured the perimeter, implemented roles and instituted the Principal of Least Privilege, what's next? You must have a plan to recover from a system failure, compromise, or unauthorized change. Data preservation is the actions necessary to successfully perform that recovery operation. The best recovery operations are:

- Documented: A step by step SOP is available. Memories sometimes fail and steps are missed in times of crisis. This also provides a learning library if the responsible person changes.

- Practiced: A procedure well documented, but not practiced can be a disaster waiting to happen. Computing environments change routinely. Minor changes may affect the viability of your backup and restore plan. Practicing them on a regular basis helps to identify these issues when your personnel are not in crisis mode. When practicing, attempt to restore files and data to test locations as not to overwrite production information (in case there is a flaw in your procedure). Document all practice attempts, lessons learned, and update your procedures as a result. (e.g. restore the X directory from backup quarterly)
- Store Data using the 3-2-1 rule: The 3-2-1 rule states that you should:
    - 3 – Have Three Different Copies of the Backup: If you are restoring from a backup, you must consider that this may be in a time of crisis. Ensuring you have copies of your backup provides protection in case you accidently damage or destroy the original backup.
    - 2 – Use Two Different Media Types. If you store all three copies of your backup on the same external drive and it fails, is destroyed (e.g. a fire), or is stolen, then your efforts are wasted. By backing up to two different media types, this helps to ensure failure or loss of the primary doesn't prevent restoration of the data. If you backup to a hard drive then burn at least one other copy to tape or DVD.
    - 1 – Store One Copy Offsite. This prevents the accidental destruction or theft of the data from preventing restoration. When storing the data off-site, you must ensure its protection. If storing physical media backups store them in a locked fireproof container. Another solution is to use a cloud-based offsite encrypted storage solution such as Carbonite or another solution provider. Not all providers provide the same services, so shop around.

User Education: All your best efforts are wasted if your users do not understand their roles in protecting your information. Every business is different. The policies and rules you have for web access, email usage, and what you consider appropriate may be completely different from another business. Consider the development, update, and monitoring of:

- Published Policies: Not only are these potentially a regulatory requirement, but also a best business practice. Your policies should be clear and concise rules for conduct. They should encourage employees to seek clarification when needed and ensure they are internally available for their easy reference at all time. If employees fail to adhere to these policies, they can be used by your HR team to terminate the employee for cause.
- Employee Acceptable Use Acknowledgement: Develop a written notice of conduct when utilizing your information resources. Clarify the use of the internet and email for personal use as applicable. Clarify the introduction of software, requirements for its install or use, and what the procedure are for approval. This document should directly reference you published policies and any regulatory guidelines as applicable. Have each employee sign the notice at a minimum upon hire, although it's a better practice to re-acknowledge the policy annually. This keeps the

ruled fresh in the minds of the employees. The SANS Institute has a sample Acceptable Use Policy available that can be used as a starting point.

- User Training: The cost of training your users to be safe while using your information resources is far less inexpensive than disaster recovery resulting for a breach. This training can be as simple as an in house presentation to remind users of their role in protecting the data. It should be an open conversation, free from senior management presence. Its far better to training, identify, and correct behaviors before they become a problem, then discover non-compliance after the fact. When possible make the training fun and provide scenarios and group activities to engage your staff. KMBL security provides a sample training presentation you can use as a baseline.

If you implement these seven areas outlined in this paper, you can significantly lower your risk of information compromise. These steps can be complex and require much thought and preparation to properly implement. When possible, engage a group of employee stakeholders to help determine the best practices and implementation strategies for each area. This will provide the overall best product and lower the overall effort. Just remember, your information security is only as strong as your weakest link.