Global Information Assurance Certification Paper

Nurturing Corporate Security – A Mundane Reality

Rick Jensen
December 30, 2000

The Landscape

An intrusion occurs in the corporate network. Management wants security tightened yesterday. The usual suspects are rounded up. Statements explaining the incident cloak the reality - security is not revenue producing. Let's face it, the chances of discovering Tom Cruise dangling from a trapeze in the computer room is nil. So much for help from Hollywood. In fact, allocating resources to network security can be career limiting. Executives of many organizations still operate in denial, naively, or are unwilling to assess network security and remain entirely focused on profits and revenues.

Pick up your favorite industry weekly. There will be one or more articles on security products, services, or hacks. Now look for some guidance on convincing management that a policy based program and resources are needed. While we are deluged with information describing exploits and explaining security strategies, little advice can be found on navigating corporate corridors, engaging management in creation of a security program, publishing policies, or obtaining resources for security in an unaware corporate environment. The real security challenge may be cultural and organizational NOT technical.

The Computer Security Institute /FBI Computer Crime and Security Survey revealed electronic attacks resulted in $266 million in losses at 273 U.S. organizations for the year 2000. Except for the banking industry, U.S. legislation is primarily targeted at the punitive process not the preventative. The rest of the world is in the same situation. The UK has launched the Turnbull initiative requiring publicly traded companies to reveal evidence of risk control measures as part best operational practices. However, there is ample room in the initiative reporting requirements to neutralize the intended results. Legislation offers no relief.

What is the corporate culture? Is short-term profit a significantly higher priority than long-term sustainable growth? Does management believe that buying and installing a firewall is adequate? What are the risks IT is asked to accept? Are acceptable risks defined by how much damage can be sustained without affecting the bottom line? Has management been alerted to current and potential operational risks or would such a report be filed under acceptable risk? Are executives leary from stories of updates that bring systems down causing problems rather that improving operation?

Commenting on the viability of the SANS Top 10 Security Risks, Robert Rosen, Director of Research for the U.S. Army, observed "I have noticed how non-exotic the list is". While exploits of vulnerabilities can be truly exotic, taking action to make a network more secure is not. In fact, raising management's awareness of the need for security is

achievable. Below are some ideas on the subject.

Promoting Network Security and Becoming More Secure Now

1. Sell network security as a business tool – not a preventative measure.
Security becomes an operational reality in corporate cultures operating in denial only when an intrusion takes place. No action will be taken until it is needed and then it is demanded yesterday. Even then, living in denial can sometimes persist. The audience for security among management is non-existent. Network security must be sold as a tool for risk management and sustained growth NOT as what-if-insurance.

Frame network security in business terms and executive-speak. Conduct a cost-benefits analysis. Gather operational plans, mission statements, and business requirements from business units. Align security measures with business unit goals. Calibrate the magnitude of pain if email or other major resource were to be disrupted. Determine the operational cost of an outage as well as the recovery cost. Assign dollar figures to time, labor, coordination effort, rescheduling and delay of other projects for recovery and restoration of critical services. Use the costs derived from the analysis to build a case showing minimizing risks and impact of disruptions is a tool for increasing the likelihood of meeting business objects.

Portray the security program as a tool to mitigate loss of revenue and increased operational costs due to disruptive events. Cost-benefits analysis moves security from the guilt-based "you'll be sorry if …" onto the list of objective business tools used to maintain revenue and meet operational goals. Find out if insurance premiums are reduced where network security policies and programs are in place. Decreasing the cost of operational necessities like insurance is almost as good as bringing in revenue. See item 6 for other angles.

2. Find or recruit an executive sponsor.
Regardless of the worthiness of the cause, security might remain in dreamland if effective communication with decision-makers is lacking. Those operating in a lax security environment understand that a process is needed. It's not something you run out and buy. Unfortunately, it's not a pill. A policy-based process is needed. Establishing that process will impact the corporate culture making a request for a security program easy to ignore or marginalize.

Gaining attention of executives requires a sponsor. Find and development a relationship with a sponsor. A sponsor is one of the corporate movers and shakers. A sponsor participates at the highest levels of decision-making. A sponsor can put network security on agendas and get the talk started. A sponsor can offer advice on which approach will be well received and who among management is receptive to the network security cause. A sponsor can help recommend the actions most likely to succeed from suggestions. A sponsor can identify key motivational factors among the executive staff and prepare opportunities to build security awareness and their proper timing in the mix of corporate plans and events.

Ideally, this sponsor is the CIO. If not start with a list of the company officers. It may be the CFO, who pays the insurance premiums; the CTO, who may be a long-term thinker; or the COO, who sees the organization function on a day-to-day basis.

Build security awareness with the sponsor. Share security issues with the sponsor. Help the sponsor see the picture within the current corporate environment. Ask the sponsor to help with the cost-benefit analysis.

3. Prioritize Security Efforts Via the 80:20 Rule.
A project cliché, 80% of the goal is attained with a 20% effort, completing the remaining 20% is 80% of the effort. Not intending to trivialize security complexities, the 80:20 rule can be used to make two action lists.

A 20% effort list for immediate action:

- Create a strong password for your own system.
- Turn off unneeded services.
- Deploy new systems with security features enabled.
- Write a recovery plan.
- Disable null sessions.
- Delete guest accounts.
- Encrypt critical files.

An 80% effort list that will require planning:

- Create, publish, and deploy a security policy.
- Deploy an intrusion detection system.
- Add a DMZ to the enterprise architecture.
- Develop secure external access to internal systems.

Refer to the SANS top 10 list for additional items.

4. Deploy Security in Conjunction with Operational and System Transitions.
Take a page from the congressional playbook. Congressmen arrange for riders to legislation in exchange for votes. The network security version of this is adding stronger security during OS upgrades, when launching new applications, during office moves, or other transitions. For instance, put the 20% effort list into action when upgrading operating systems. Indicate that these measures are required for the upgrade, new application, server, OS etc.

Obviously a direct dialogue and agreement with management is preferred but in its absence this alternative may prove helpful.

5. Secure your machine now.
Most likely, you don't need anyone's OK to secure you own system. Take the list from

item 3 and apply it to your own system. Make strong passwords, configure the system to require password changes every 60 days or so, install a personal firewall, determine which of your files are candidates for encryption, turn off anonymous logons and null sessions. You'll experience first hand the inconvenience of creating a secure password every 60 days. These are actions that will be required of all users when a program is approved. They are easy to perform but not always easy to live and work with. Have direct reports secure their machines and listen to the gripes. Are post-it notes with passwords getting stuck on monitors?

6. Create policies and procedure and seek their approval.
Give management a framework to review and approve. Make the pitch. This requires some detective work to create a favorable opportunity and collaboration with the sponsor. Calibrate the individual attitudes towards security among the executive staff, and identify barriers perceived by management. Design the policy framework to match the corporate culture and align it with operational goals as stated earlier. Presenting a full-blown plan that will be rejected isn't realistic and might imply that resources are being used on non-critical actions.

Management may not know what needs to be done or what is required to establish an operationally effective process until an outline is offered. Explain the 20% effort list and demonstrate that progress is achievable and believable.

7. Secure each new system built and staged for users.
As systems are built and staged for users deploy them with security features. Create strong passwords, for instance. Avoid the use of "password", "hello", "welcome" etc. in order to get a user up and running sooner. Sure, simple passwords are easy to remember but the practice sets lax security as an expectation among users. Using a strong password sets an example and demonstrates that security is of value and is required. A password generator can be used. Several are freely available online.

Staging new systems is another opportunity to deploy the 20% effort list. Make a disk image or registry snapshot for future recovery or as a baseline to test for revealing malicious activity. Beef up the strength of screen saver and turn them on during deployment.

Build awareness and give security a boost with executives and their admins by employing techniques like generating a strong password from a favorite phrase etc. Demonstrate that effective security does not have to be onerous for users.

8. Keep security skills current.
As mentioned above, understanding the cultural impact an organization may experience to become more secure can reveal ways to promote security as a business tool. Before asking others to comply with security policies make sure there is adequate proficiency deploying security skills. Do some of the following:

- Make backups and practice restores. How long does it take? How reliable is the backup system?
- Turn on event logs. How fast do the log files fill up? What tools are available to scan log files? Which event patterns indicate trouble?
- Keep an operational journal and record security related events and their impact.
- Practice incident response scenarios.

Respond that these activities are used to help gauge operational bandwidth as well as increase security. Let management express concerns but avoid I-told-you-so's if or when an incident occurs. Remember, management should see security as a business tool.

9. Acquire basic vulnerability assessment skills.

Executives may have a "show-me" attitude. They may subscribe to one or more myths surrounding network security and be under the impression that current measures are adequate. Get a book – "Hacking Exposed" for instance. Find websites that publish exploits. If possible, assemble a small test network for test and demonstration purposes. Assemble a tool kit. Many tools are free or have no-cost demo versions that are functional. Learn about methodologies and tools for the most likely exploits your network might face. Subscribe to security related online newsletters.

10. Ask permission to conduct a vulnerability assessment.

Exploiting the network is risky business. Before executing an exploit on a production system get written permission. Asking for permission to conduct exploits and a vulnerability assessment is a pretty quick way to calibrate management's attitude towards network security.

In one instance where permission was granted, a user with no administrator privileges or detailed network knowledge was given permission to conduct a vulnerability assessment. The assessment discovered that some measures were in place, but audit logs were not reviewed and no monitoring operations were in place to alert system administrators of the intrusion attempt. Persistence and a little luck allowed unauthorized administrative access to the primary domain controller, passwords, and other sensitive information. Not only was the exploit successful, but IT never knew it took place.

11. Focus the effort.

If the organization is not ready for an all out network security program, volunteer as a project team member on a project requiring security. Reach an understanding with the project leader that security measures will be part of the project deliverables. Narrow the scope so that success is achievable and security can be seen as an enabling function for confident, secure operation. Track the progress. Measure the incremental cost of security. Add the information to the cost-benefit analysis. Use projects to spread the message about process of security.

Conclusion

This paper has offered some thoughts for IT management and staff on ways to cope and survive in a corporate culture that is still in denial concerning the benefits of the security process. Many of the suggestions could be familiar. None of them are exotic.

Be advised that some suggestions may come with career related risks. Adopt them to the corporate culture when prudent and practical.

If all else fails develop a recovery plan.

Resources for network security may never materialize. On the other hand, management could beg for a plan and offer funding and resources for a program. In either case, create an incident response plan now. It should be high level, simple, and match the current level of security awareness. The following steps might be included:

- Identify resources that can be exploited.
- Prioritize the resources by level of criticality.
- Neutralization of the intrusion.
- Estimate time needed to recover and restore resources.
- Explain recovery of resources.
- Describe restoration of services.

The plan won't make security stronger but if or when an incident the situatioin will be more manageable and perhaps the planned response can be a catalyst to call attention to the need for a security program. More importantly, a tool will be available to manage expectations and panic during an unforseen incident.

References

Robert Rosen, eSeminars. "Security Vulnerabilities". http://www.eweek.com (November 2, 2000).

The SANS Institute. "How to Eliminate The Ten Most Critical Internet Security Threats." Version 1.31, December 28, 2000. URL: http://www.sans.org/topten.htm (29 December 2000).

The Institute of Chartered Accountants in England & Wales. "Internal Control – Guidance for Directors on the Combined Code". (AKA, Turnbull Initiative.) September 1999. URL: http://www.icaew.couk/internalcontrol (7 November 2000).

NT Security Issues. A collection of various articles on NT Security. URL: http://netsecurity.about.com/compute/netsecurity/cs/ntsecurityissues/index.htm

Computer Security Institute. "Computer Crime and Security Survey." December 2000. URL: http://www.gocsi.com/prelea_000321.htm

John Taschek. "Managers Freakier … than hackers". eWeek 11/13/00

InfoWorld. "Security In Depth, 5 issues to think about when building your strategy".

November 13, 2000, Volume 22, Issue 46.

Last Updated: September 25th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event