HOW TO SUCK AT INFORMATION SECURITY

This cheat sheet presents common information security mistakes, so you can avoid making them.

Security Policy and Compliance

Ignore regulatory compliance requirements.

Assume the users will read the security policy because you've asked them to.

Use security templates without customizing them.

Jump into a full-blown adoption of frameworks such as ISO 27001/27002 before you're ready.

Create security policies you cannot enforce.

Enforce policies that are not properly approved.

Blindly follow compliance requirements without creating overall security architecture.

Create a security policy just to mark a checkbox.

Pay someone to write your security policy without any knowledge of your business or processes.

Translate policies in a multi-language environment without consistent meaning across the languages.

Make sure none of the employees finds the policies.

Assume that if the policies worked for you last year, they'll be valid for the next year.

Assume that being compliant means you're secure.

Assume that policies don't apply to executives.

Hide from the auditors.

Security Tools

Deploy a security product out of the box without tuning it.

Tune the security event management tool to be too noisy, or too quiet.

Buy security products without considering the maintenance and implementation costs.

Rely on anti-virus and firewall products without having additional controls.

Run regular vulnerability scans, but don't follow through on the results.

Let your anti-malware, log management, and other security tools run on "auto-pilot."

Employ multiple security technologies without understanding how each of them contributes.

Focus on widgets, while omitting to consider the importance of maintaining accountability.

Buy expensive product when a simple and cheap fix may address 80% of the problem.

Risk Management

Attempt to apply the same security rigor to all IT assets, regardless of their risk profiles.

Make someone responsible for managing risk, but don't give the person any power to make decisions.

Ignore the big picture while focusing on quantitative risk analysis.

Assume you don't have to worry about security, because your company is too small or insignificant.

Assume you're secure because you haven't been compromised recently.

Be paranoid without considering the value of the asset or its exposure factor.

Classify all data assets as "top secret."

Security Practices

Don't review system, application, and security logs.

Expect users to forgo convenience in place of security.

Lock down the infrastructure so tightly, that getting work done becomes very difficult.

Say "no" whenever asked to approve a request.

Impose security requirements without providing the necessary tools and training.

Focus on preventative mechanisms while ignoring detective controls.

Have no DMZ for Internet-accessible servers.

Assume your patch management process is working, without checking on it.

Delete logs because they get too big to read.

Expect SSL to address all security problems with your web application.

Ban the use of external USB drives while not restricting outbound access to the Internet.

Act superior to your counterparts on the network, system admin, and development teams.

Stop learning about technologies and attacks.

Adopt hot new IT or security technologies before they have had a chance to mature.

Hire somebody just because he or she has a lot of certifications.

Don't apprise your manager of the security problems your efforts have avoided.

Don't cross-train the IT and security staff.

Password Management

Require your users to change passwords too frequently.

Expect your users to remember passwords without writing them down.

Impose overly-onerous password selection requirements.

Use the same password on systems that differ in risk exposure or data criticality.

Impose password requirements without considering the ease with which a password could be reset.

More Security Mistakes

The 10 Dumbest Things People Do...
http://www.sans.org/newsletters/ouch...

10 common security mistakes...
http://www.techrepublic.com/blog/10-things...

Mistakes ... that Lead to Security Breaches
https://www.sans.org/security-resources/mistakes...

Authored by Lenny Zeltser, with contributions from SANS Internet Storm Center handlers. Lenny aims to help enterprise and home users avoid making information security mistakes and publishes advice at zeltser.com/blog. Creative Commons v3 "Attribution" License for this cheat sheet version 1.4. For more cheat sheets, see zeltser.com/cheat-sheets.