IT Audits: Prevention and adequate security can save you a lot of money and trouble

*In today's interview, **Jan Krátký**, Managing Director at the IT division of ICS Praha, talks about IT audits and their benefits for organizations.*

Q: Let's talk about IT audits for a while. I guess the first question has to be: What benefits can I expect to get from an IT audit?
A: There are many benefits but the ultimate purpose of IT audits is to save you money. Process audits allow you to work more efficiently, thus reducing overheads and IT expenses. Security audits, on the other hand, give you peace of mind knowing that your infrastructure is not vulnerable to potential threats. As an efficient preventative measure, they can save you lots frustration and firefighting expenses. What's worse, major security incidents may hurt your reputation as a good business partner, potentially resulting in much higher indirect losses.

Q: I see. You mentioned process and security audits. Can you briefly explain the differences?
A: Simply said, there are two main audit types. You can examine either the efficiency of IT processes or infrastructure security. Process oriented audits focus on an enterprise's applications architecture, including the data links between different entities, systems and processes. However, they consider other areas as well, such as internal processes within the in-house IT department.

Security focused audits include an exceedingly broad scope of areas and activities intended to cover a wide range of potential risks and threats – from assessments of computer network vulnerability to penetration testing, social engineering to physical security. The latest area often involves also building security tests, access control systems and so on.

Q: Speaking about risks and threats, how does one assess information infrastructure vulnerabilities?
A: Obviously, risk assessment is an integral part of every audit and its deliverables. Auditors can use different criteria depending on what is most appropriate in each specific instance. That being said, the assessment is usually based on potential impacts on the client's core activity and credibility in the eyes of its clients and business partners.

Q: You mentioned earlier that IT audits and their follow-up are a great way of saving money. Can you be more specific? And is it possible to quantify these benefits?
A: Speaking of process and infrastructure optimization, the benefits can be usually assessed quite accurately. Security audits, on the other hand, are usually not concerned with saving money directly – at least not primarily. Their main objective is to minimize potential risks and threats. Security incidents can inflict significant losses and damage; there were even cases where a major security breach proved to be lethal for the organization. Therefore it is only wise not to neglect prevention. It may sound cliché but when the chips are down, it's always better to be safe than sorry.

Q: And to get there do IT audits have to take place regularly? How often?
A: Again, we have to distinguish between the different audit types. Process optimization audits usually need not be repeated for quite a long time – unless, of course, the organization goes through significant organizational changes. Security audits, on the other hand, should be conducted on a regular basis. IT security is a constantly changing and rapidly developing field. The nature of potential threats and attacks evolves very quickly. Therefore, we recommend to repeat the basic tests at least on a yearly basis.

Q: Security and data protection are one of the key IT audit drivers. Have you noticed any changes in how your clients see this area?
A: In the past, many Czech companies did not attach much importance to IT security. Usually, this laissez-faire attitude changed with the first significant security incident – but the late U-turn usually entails considerable financial cost and credibility losses.

Anyhow, the good news is that the situation seems to be improving. Today, even small and medium-sized enterprises appear to be taking security seriously.

Q: Last years have seen a steep rise in the popularity of virtualization and cloud computing. How do these concepts impact enterprise data security?
A: Indeed, both virtualization and cloud computing have been big game changers, effecting a significant shift in how enterprises use their information technology. This often poses many new challenges to the organization's IT department. Bear in mind that renting a piece of software or a cloud service from a respected provider does not ensure sufficient security in and of itself. Particularly hybrid systems, that is systems combining cloud based and locally operated solutions, have significant security requirements to be catered for.

Q: Security audits do not cover just data security. What other areas are normally examined?
A: The scope of security audits is very broad. An audit may involve for instance vulnerability or penetration tests to assess how resistant an information system is to potential attacks from the Internet or local area network. In addition, audits typically include also physical security checks to test the efficiency of access control measures preventing unauthorized access to buildings, data centers, server rooms and other restricted premises. The most important or potentially vulnerable areas to focus on are always determined in advance during initial discussions with the customer.

Q: How do Czech business fare in terms of data security compared to their foreign counterparts?
A: Frankly speaking, Czech businesses have been rather neglecting security and have a lot to make up for in this area. That being said, the situation has improved significantly over the last couple of years. To a certain extent, this positive development has been driven by several outside factors, such as the Cybernetic Security Act.

Q: Why should organizations commission external suppliers instead of handling the audits internally?
A: The reasons are quite straightforward. Some tests, such as black-box vulnerability testing, assume that the attacker has only a minimal knowledge of the target infrastructure and cannot be performed internally. Interestingly, such tests often provide priceless information on vulnerabilities which could be potentially exploited by any attacker on the Internet.

Moreover, the amount of work in many smaller and medium-sized enterprises is simply not high enough to hire an in-house security specialist. Employing such an expert would be inefficient. To help these organizations, we offer the possibility to hire a security specialist part-time. This allows you to use the services of a first-class security expert for just a fraction of what you would have to pay if you decided to hire a similarly skilled resource on a full-time basis.

Q: What are the deliverables during an audit? Do you describe the observations and findings only or do you, for instance, provide also suggestions as to what improvements can be made?
A: You are absolutely right. Every audit report contains also a set of possible risk mitigation measures. Most clients also immediately ask us to help with their implementation.

Q: How long have you and your company been doing these audits?
A: Well, our first audit dates back to 2003. Since then, we have helped many customers and managed to assemble a team of extremely skilled security professionals.

Q: I know that audits are intended mainly for companies. But can you be more specific? Who is the typical customer for this service?

A: In case of audits our clients are usually medium-sized and larger companies from many different fields of business. However, what with growing security awareness and requirements, the share of smaller companies has been rising steadily.

Q: Finally, can you give us some examples – a successful audit and the benefits it brought to the customer?

A: Unfortunately, I have to disappoint you. I cannot talk about any specific results or findings, because this information is highly sensitive and intended for the client only. Every audit contract includes a strict confidentiality clause in which we undertake not to disclose the findings to any third party. However, we fully understand that this information is very relevant for organizations considering an IT audit. Therefore, we have prepared samples of how audit deliverables look like and what our customers and prospects may expect to get.

Interested in IT audits? Request your free report sample or additional information today at kratky@icspraha.com.

About the Expert

***Jan Krátký** has worked as developer and IT specialist since 1996. For more than 14 years he has been Managing Director at the IT division of ICS Praha. As a leading IT consultant, Jan helps his clients to find the right solutions for their needs, focusing in particular on security, communication and project management. In addition, he is a certified expert on computer networks running Windows or Apple hardware.*