Ask The Experts!

Brad Bauman, P.E., ASQ-CQA, VMEC Professional Manufacturing and Business Growth Advisor
bbauman@vmec.org/ (802) 353-6836

QUESTION: Why should I care about the security of my enterprise data?

MY ANSWER: Let's face it, in this day and age, data is stored and transmitted for nearly every transaction we make. Whether it's a gasoline purchase, a doctor's visit, or a mortgage application, data gets collected, transmitted and likely stored indefinitely. MarketTechBlog.com states that 2.7 zetabytes of data exist in the digital universe today. With the existence of all this data, it's no wonder that identity theft is on the rise. Last year alone, over two million complaints of identity theft were reported in the U.S., according to the Federal Trade Commission. And personal data is not the only thing at risk; corporate espionage is also on the rise causing the loss of sensitive data such as client lists and intellectual property.

Why should we care? The answer to that question is a bit overwhelming. According to The Epoc Times www.theepoctimes.com:

> *Economic espionage represents "the greatest transfer of wealth in history," said General Keith Alexander, NSA director and commander of U.S. Cyber Command, at the American Enterprise Institute in 2012.*
>
> *BlackOps Partners Corporation, which does counterintelligence and protection of trade secrets and competitive advantage for Fortune 500 companies, estimates that $500 billion in raw innovation is stolen from U.S. companies each year. Raw innovation includes trade secrets, research and development, and products that give companies a competitive advantage.*
>
> *"When this innovation is meant to drive revenue, profit, and jobs for at least 10 years, we are losing the equivalent of $5 trillion out of the U.S. economy every year to economic espionage," said Casey Fleming, CEO of BlackOps Partners Corporation. "To put it into perspective, the U.S. will take in $1.5 trillion in income taxes and $2.7 trillion in all taxes in 2013."*

Is your company's data at risk and is there anything you can do to reduce the risk of a loss of sensitive data? The answer to both questions is **yes**. Whether it be a threat from an overly ambitious teen hacker, a disgruntled employee, or a full on attack from a foreign military cyber unit, your data is at risk. While there is no way to 100% guarantee data security, you can implement an Information Security Management System (ISMS) that will greatly reduce the risk of data loss and at least inform management of their total risk. One such ISMS is **ISO 27001**. Designed to closely align with ISO 9001, companies that are already ISO 9001 compliant will find that complying with ISO 27001 is relatively easy. ISO 27001 compliance ensures that your security arrangements are fine-tuned to keep pace with changes to security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO 27001's flexible risk-driven approach as compared to, say, Payment Card Industry Data Security Standards (PCI-DSS).

So how does ISO 27001 work? ISO 27001 begins with a comprehensive, self directed, risk assessment. From this assessment, controls are self imposed to mitigate risk. If mitigation is not practical, the standard offers three other options for dealing with risk.

Avoid – do not to accept online credit card payments

Transfer – use of cloud based services

Accept – management accepts that a meteor strike could cause data loss and simply chooses not to mitigate this risk

After controls are in place to mitigate risk, the organization monitors the effectiveness of its ISMS and continuously improves the system as needed.

Does your company need ISO 27001? To answer this question, you might want to consider the following. Has your website ever been hacked? Have you ever experienced data loss? Has intellectual property ever "walked" out the door? Do you know the answer to these questions? ISO 27001 can help with all of these issues.

If you'd like to learn more about ISO 27001, you should start by downloading a copy of the standard at the link here and if you have further questions, please don't hesitate to contact me at any time.