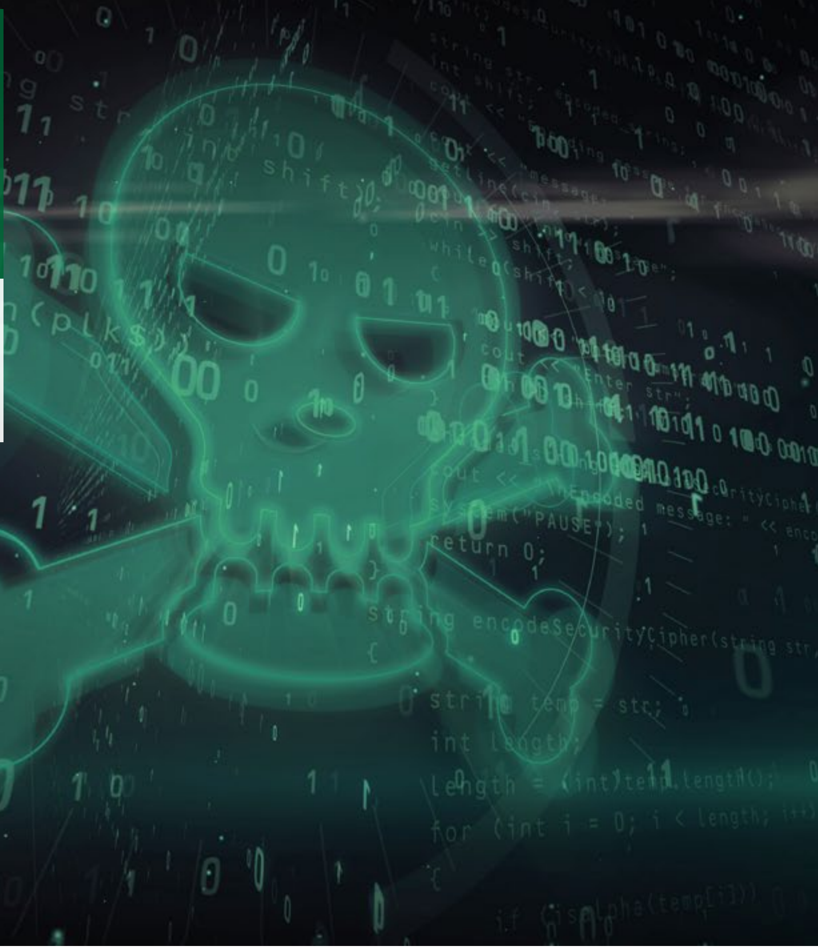
Whitepaper — INFORMATION SECURITY: THAR BE MONSTERS!

DEKRA


DocumentType()
then
return 0;
string encodeSecurityCipher(string str
string temp = str;
int length;
length = (int)temp.length();
for (int i = 0; i < length;

Every individual, organization, and business using technology has skin in the game when it comes to matters of information, computation, and data security.

by Neil Simons, Information Security Regional Excellence Manager, DEKRA Audits

A business has an obligation to protect itself, its customers, its partners, and its stakeholders. While we all believe the risks are known and the potential impacts are understood, there is a tremendous gap in the marketplace and with technology to keep up with or to get ahead of the risk and impact of cyber threats that encompass the reality of today's technology, social, computing, and business environments. In short: Yes, there are monsters thar.

According to Forbes, cyber crime and poor technology and data stewardship will cost businesses $6 trillion globally and $600 billion in the US alone. CNN Money reports that, in 2019, it will cost the average American large corporation $15 million. Poor stewardship can also cost your organization its reputation, its operations, its customers, its investors, and increasingly open the organization to legal liability through both regulation and potential litigation.

In the news and within our business circles, there are constant reminders and examples of breach (actors seeking access and control though exploitation), improper management (failure to protect), or just plain human error. The lesson is that it is vital that every organization take a position to put in place the combination of programs, processes, technologies, and culture through the creation, execution, certification, and maintenance of a certified Information Security Management System (ISMS) within their businesses.

A comprehensive systems strategy serves to protect not only consumer information, but also infrastructure, data, and operations capabilities. Furthermore, it provides a level of legal protection to the organization.

We have already witnessed complete healthcare systems, including hospitals and direct patient care, taken hostage through ransomware; we have seen the protections placed by international custodians of consumer financial data breached with tens of millions of consumers' data (including unique identifiers like social security numbers, dates of birth, and banking PINs) placed for sale on the dark web to actors unknown. According to Forbes, Marriott's fines under GDPR will surpass $8.8 Billion USD for their failure to protect data.

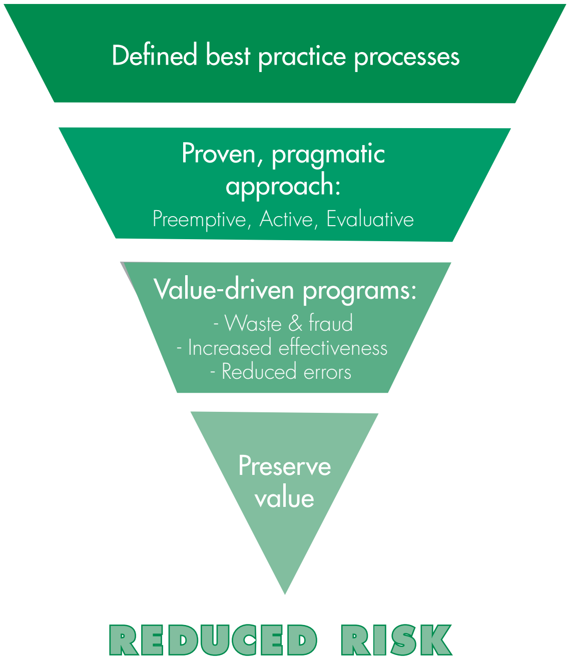
We have seen infrastructure exploited to breach data and interrupt vital infrastructure and services. The list is only going to continue to grow. Each event further diminishes the confidence we place in the technologies upon which we rely.

The fact of the matter is that everyone's data, everyone's systems, and everyone's business is at risk of exposure. If we accept that there is no way to prevent it, the questions and challenges become: How do we put in place the programs, policies and technologies to manage Information Systems technologies to demonstrate the highest degree of accountability for the preparation for an incident? How do we prepare our organizations to do the "right" things before, during, and after an IT security event?

This is where the strategy of developing and managing an ISO 27001-compliant Information Security Management System (ISMS) can help to prevent against and guide through protection and safety events. Under such a program, a certified organization can offer proof to their customers, their associates, their industry, and regulatory bodies that they have done their duty in protecting these assets to these internationally-recognized standards.

That your organization, your partners' organizations, or your customers' systems will be impacted is practically a given in today's environment. In that case, what does an ISO 27001-certified management system offer you? To answer this, let's examine what exactly an ISMS does.

IT and Information Systems are not most organizations' core business. The manufacturing, healthcare, retail, aviation, and automotive industries may be technically savvy, but in essence they use these technologies in support of their core business functions. One of the most significant trends in small and midsized business operations is the increasing outsourcing of information technology services to third parties. An ISO 27001-certified Information Security Management System is an indicator to the market these organizations serve that their environment provides their customers with defined best practices; a proven, pragmatic approach; value-driven programs; and preservation of value.


Defined best practice processes
Proven, pragmatic approach:
Preemptive, Active, Evaluative
Value-driven programs:
- Waste & fraud
- Increased effectiveness
- Reduced errors
Preserve value
REDUCED RISK

What Are the Choices For Management?

Let's take a look at what is being done in the market today. There are a few current strategies being pursued:

Ostrich Strategy: "We're not big enough, don't have millions of customer files or proprietary information to be a target so it's irresponsible to spend the resources to prevent the inevitable". This has proven to be a disastrous strategy in IT management. Target paid $18.5 million dollars in fines alone for the 2013 breach of their retail/POS systems which affected 41 million customers. The source of this attack and breach was the perpetrator gaining access via a small supplier of HVAC services to the organization. While it has taken years for Target to recover the lost customer confidence and their customers have had to face the possibility of identity theft, it is also true that that small HVAC supplier is no longer in business (over 150 jobs lost) as a result of the negative publicity and litigation that followed the events.

Reactive Strategy: Another strategy being followed by many organizations, the one probably being pursued by the majority of organizations is to only prepare processes, procedures, and practices to respond or recover from an attack. This approach presumes that there is an "acceptable loss" of data and operations capability that is acceptable to the business. As long as there is a way to effectively recover afterwards, then there is "no harm, no foul" and that a given incident is simply an expected "bump in the road". In some cases, this may be an appropriate approach to the challenge; however, it leaves the business and their systems exposed.

Point Solutions Strategy: The most commonly used strategy is one of addressing IS and IT security with "point" solutions: independently addressing specific areas through the execution of controls of some form, such as the creation of simple policies, by backing up systems and data, by providing technology such as endpoint protections (virus and malware scanning) or creating monitoring for network and systems activity through Security Information and Event Monitoring (SIEM) solutions or the establishment of a SOC (Security Operations Center). While taking strides forward in action activity and investment, these solutions leave many significant gaps within an environment that leave the firm vulnerable with risk and and increased liability.

Comprehensive Strategy: In the minority are those organizations who have, either by mandate or through negative experience, learned that the only way to meet the challenges of IS/IT security (and through that the enhancement and assurance of safety and security within their ecosystem) is to design and implement a comprehensive managed solution within their business. These management systems should include the primary pillars of the best practices of Quality Management.

Global InfoSec Standards

Among the ISMS standards in the marketplace, there is only one that is a genuinely global standard constructed and accepted worldwide, ISO 27001. Within an ISO 27001-compliant management system, other standards or acts, such as NIST, DoD, and even GDPR (the 2018 law that determined the EU data management minimum standards), can be integrated and included within the controls managed.

Maintaining compliance to these standards is not a simple matter for any organization seeking to manage the information security concerns facing them. ISO systems offer the historically proven depth, breadth, flexibility, and capability to be able to accommodate required external controls and processes and be extended to meet any new different or upcoming requirements and standards in the future.

Elements of ISO 27001

Within the world of ISO and ISMS the focus is on multiple organizational areas. The program and management system reaches beyond the actual technology itself. There are three elements to the ISO 27001 approach to IT and IS security:

People: People are proven to be the weakest link in IT security. An effective ISMS will directly address this. Has every employee been trained? Does your organization have clear documented policies? IT Security education and practices need to address security across every single individual, department, and function in the organization. It is the single largest point of failure in IS/IT security, and this is due to the reluctance to allocate the needed resources to education.

Process: Are your people and technologies working together to maintain the vigilance required? What happens when someone joins or departs the organization? What happens when a security event occurs? Who does what and when? What is the plan? What is the risk? The cost of not having vital security processes in place is resorting to the reactionary response to every situation. There is no best practice in addressing any given incident and there is no way for an organization to "know" how to prevent and recover from an incident without going through the processes of establishing and maintaining an ISMS.

Technology: Does your organization have in place the controls and technologies that are required to meet even the most basic security requisites? Are your routers and endpoints protected and monitored? What about whitelisting or blacklisting? Is your network traffic monitored for activity? Is your data encrypted at rest as well as during transmission? ISO 27001 helps you to ensure that both the technology your organization uses is secure and that your organization has ensured confidence (supported by both internal and independent auditing) in all of those technologies.