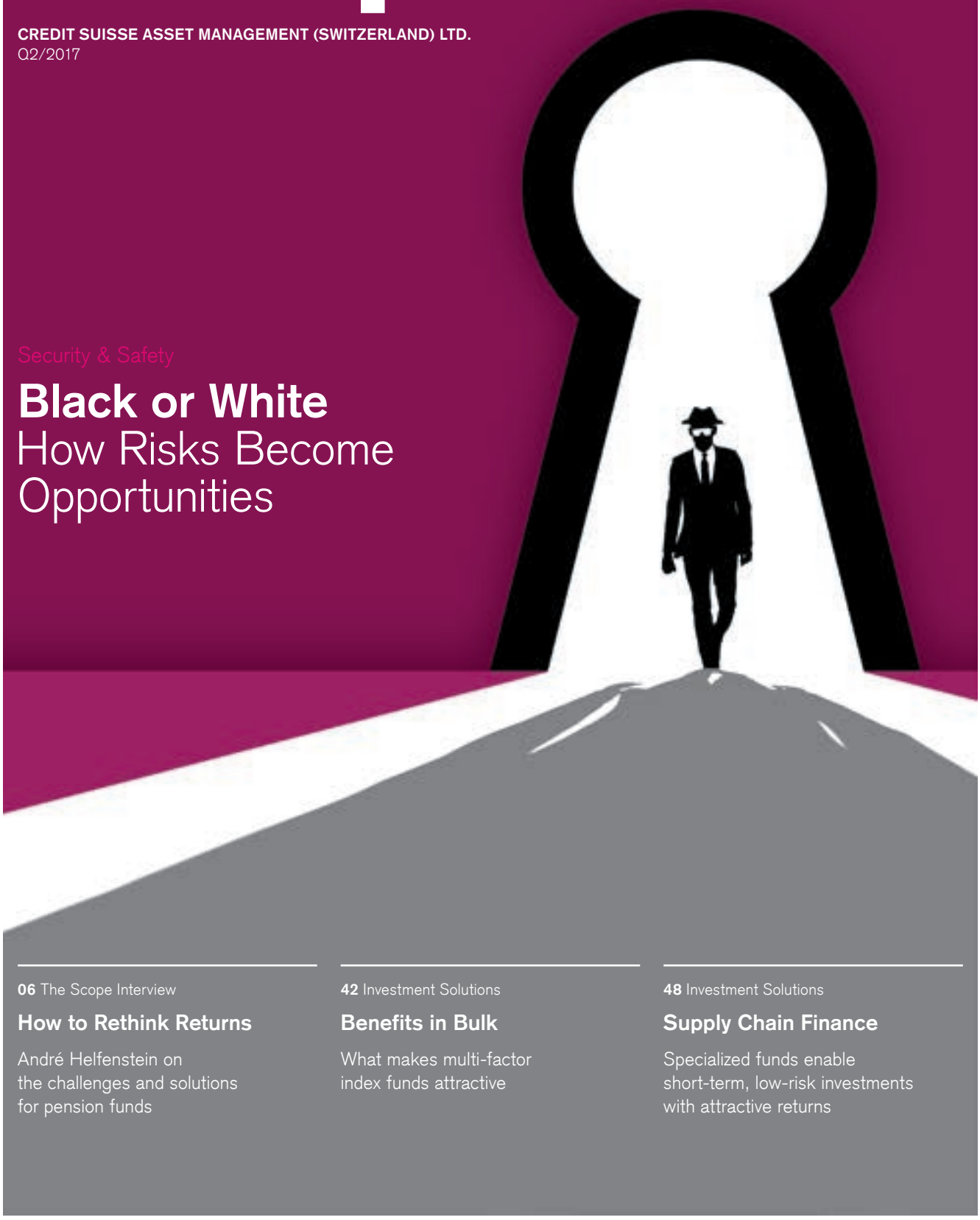
CREDIT SUISSE

Scope

CREDIT SUISSE ASSET MANAGEMENT (SWITZERLAND) LTD.
Q2/2017



Security & Safety

Black or White
How Risks Become Opportunities

075519E

Cyber Security

Dr. Stefan Frei
Security Principal, Accenture Cyber Defense
Lecturer in Cyber Security, ETH Zurich

In connecting people and machines ever more closely together, the internet has changed our lives forever. These changes are disruptive, like the introduction of the railroads and the automobile. This latest innovation is not the first to prompt critical questions regarding security and safety. New possibilities as well as threats emerge at the interfaces of technology, economy and society. What are the lessons we can draw from history?

Cyber risks are abstract, have developed slowly and, consequently, were ignored for a long time. Digital products increasingly pervade every area of life, and it is difficult to allocate resources to protect against abstract risks. These are often recognized only once a major event has occurred, with the danger of overreaction vis-à-vis defense.

Software eats the world

Software is an important driver of this development. Despite substantial investment, industry has not yet managed to create more secure software. We are still having to deal with ongoing security vulnerabilities, and now also in areas outside of the traditional software industry, which had to learn that it is impossible to prevent independent research and publication of vulnerabilities. Previously, those who uncovered vulnerabilities were ignored or prevented from publishing by means of legal redress. As a result, and despite the risks, many vulnerabilities were never patched or patched only after a long delay. Over time, the "coordinated disclosure" process became the norm: ethical researchers first privately disclose vulnerabilities to vendors and give them a reasonable deadline for developing a security update before publishing the information. If a vendor does not cooperate, the vulnerability is published immediately so that those affected by it can assess the associated risks. History teaches us that vendors will hasten to develop software updates only when faced with imminent publication. Coordinated disclosure is now established, at least in the software industry.

With the rise of the Internet of Things (IoT), many non-software industries and their products are becoming networked, often ignoring software industry best practices such as secure development and coordinated disclosure. Reports of safety defects in digital electricity meters, surveillance cameras and thermostats are increasing.

Why are digital products with preventable security defects finding their way to the market?

Lack of liability
When an innovation is introduced (e.g. the automobile, aviation), safety is secondary. Experience and safety standards are still lacking. As a technology becomes widespread, incidents increase, and society begins to ask about safety. Calls for mandatory safety standards are always fiercely resisted by the industry concerned using the same arguments:

1. The product is safe. Accidents are the fault of the user.

2. Safety standards are unnecessary. They will lead the industry to ruin.

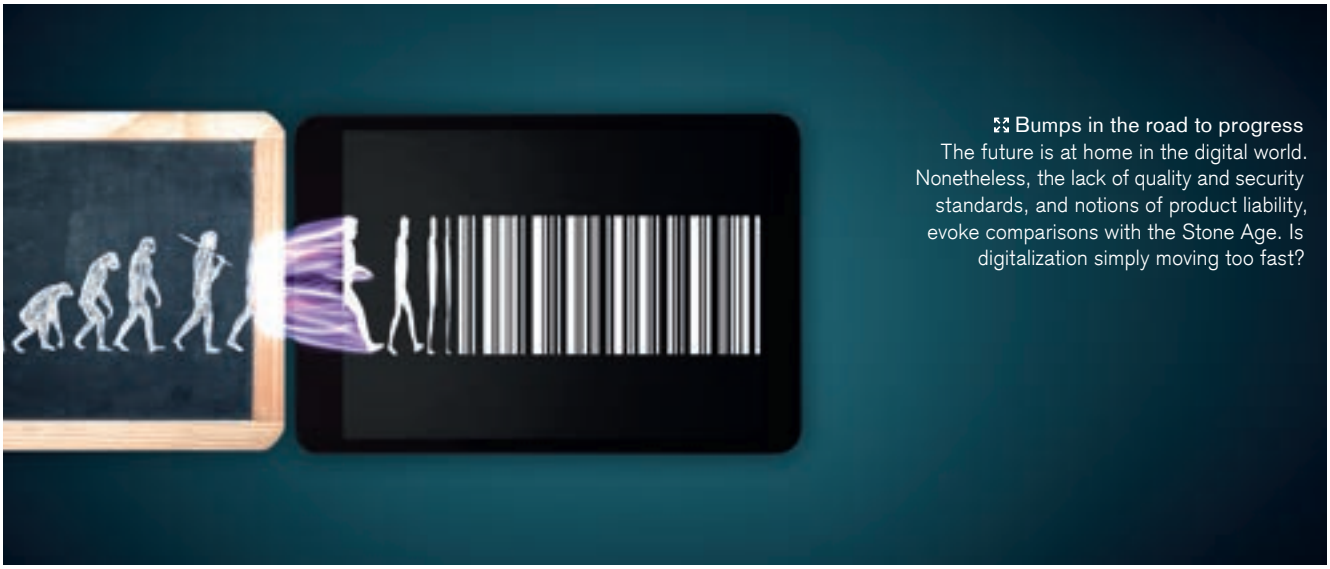
3. Safety standards will stifle innovation.

Ralph Nader's "Unsafe at Any Speed," published in 1965, illustrated this conflict and, following disputes with the automobile industry, resulted in the introduction of seat belts, crash tests and product recalls. In the early days of aviation, the industry fought against tests for aircraft engines – over half of the engines could not pass the initial test.

Today, a lack of safety standards in these industries is unthinkable. Both the automobile and the aviation industry continue to exist and are major innovators.

Where the potential for damage is great (e.g. food, pharmaceuticals, transport, construction), society has always introduced standards of quality and safety,

The sky's the limit
Cyber risks are abstract and hard to identify. In car manufacturing, on the other hand, many safety gaps are obvious, and since the publication of "Unsafe at Any Speed" in 1965, manufacturers have made great strides in plugging them. Crash test dummies provide a very useful service in this respect. The upside potential for greater security and safety in both areas is significant.



Bumps in the road to progress
The future is at home in the digital world. Nonetheless, the lack of quality and security standards, and notions of product liability, evoke comparisons with the Stone Age. Is digitalization simply moving too fast?

backed by realistic testing. Given their growing importance, the lack of such standards for digital products should be questioned.

There is no product liability for software. Security updates are viewed as product recalls for defective software at the user's expense.

Mandatory standards or tests for critical digital products must be developed, so that now and in the future the opportunities of digitalization will outweigh its risks.

Traditional vs. digital products
Traditional products rarely change after delivery, whereas digital products constantly require security updates. Many digital products have a lifetime of decades (e.g. electricity meters, monitoring systems) and replacement – e.g. when a vendor goes bankrupt – is either very difficult or too expensive. Without precautionary measures such as

- making the source code freely available (open source) as soon as the vendor is out of business
- depositing the source code with an independent party prior to purchasing it, and passing the source code to the customer once the vendor is out of business

critical products can be operating for years without protection. Many digital products are also tightly connected to the vendor's back-end services. If the back end is discontinued, a critical situation arises, for example in the case of monitoring systems. These dependencies must be taken into account prior to deployment.

Special characteristics of cyber challenges
With the dissemination of digital products, we are running into challenges that we only partially understand. Through overhasty deployment, we run the risk of causing security and safety problems that will only become evident over the long term and that will take enormous effort to correct.

As a society, we are obligated to prevent known and avoidable mistakes. Mandatory standards or tests for critical digital products must be developed, so that now and in the future the opportunities of digitalization will outweigh its risks.

Dr. Stefan Frei
For 20 years Stefan Frei has been involved with cyber security at the interface of society, economy and technology, from the perspective of both the attacker and the defender. He has worked in the areas of penetration testing, defense effectiveness, security architecture and data analytics at home and abroad. At Accenture Cyber Defense, he specializes in using threat intelligence and advanced end-to-end attack simulations to help organizations protect themselves from highly sophisticated and targeted attacks.

Accenture Cyber Defense
As one of the largest global providers of professional services for the digital transformation of companies, Accenture is a trailblazer in proactive and comprehensive implementation of cyber defense in digitalization and IT projects. In addition, it deploys more than 6,000 cyber security professionals around the world, every day. A particular emphasis is given to realistic approaches for identifying the actual and very dynamic attack vectors of cyber crime (e.g. the Internet of Things). This competence is supported through a variety of research centers and cyber fusion centers in cyber security hotspots throughout the world, such as Israel.