Ensuring Security and Prosperity
In the Digital Age
EXECUTIVE SUMMARY

Digital technologies can help China unlock meaningful improvements in economic growth and development. However, there is growing concern that as China’s individuals and small firms embrace the digital economy, they are facing cybersecurity threats beyond their capabilities. The risk is greatest in areas that will see wide adoption like the Internet of Things. China’s future prosperity will depend on the steps it takes to strengthen cybersecurity for its citizens and small- and medium-sized enterprises (SMEs).

A review of efforts by the European Union, Germany, Canada and others, shows a need to provide detailed guidelines specifically for SMEs. The history of the automobile demonstrates that to be effective, security standards for widely used technology such as the Internet of Things (IoT) should be easy-to-use and embedded in product design. Similarly, various industry consortia have and are succeeding because of a commitment to building open, flexible, and interoperable standards.

China’s new Cybersecurity Law covers important safety and security issues, but would benefit from enhanced guidance on: (1) standards for data security and identity authentication, especially for IoT; and (2) capacity-building for individuals and SMEs. The private sector can be a strong partner, provided China’s cybersecurity framework promotes common standards, interoperability, and multi-stakeholder collaboration.
I. DIGITAL REVOLUTION CAN DELIVER STABLE, LONG-TERM GROWTH

A. China is at the forefront of the digital revolution

China has a well-known history of leadership in information technology. China was printing books four hundred years before the Gutenberg press was invented. Technology innovation and knowledge sharing have always been important, but perhaps never more so than today. And China is once again at the forefront of a technology revolution – in this case, the digital revolution. Four of the world’s fifteen largest Internet businesses by market cap are Chinese. ¹ China has more than 731 million Internet users, ninety-five percent of whom connect by mobile. ² Consumer consumption is expected to reach $6.5 trillion by 2020, twenty-four percent of which will happen online. ³ It is no wonder then that China’s Internet economy as a percentage of GDP already exceeds the developed world average [Figure 1]

Figure 1: Internet Economy as Percentage of GDP (2016)
China is also well poised for the future. In 2015, China filed thirty-five percent of all robot-related patents in the world. 4 China’s digital economy is likely to create 415 million jobs by 2035, bolstering technology’s share to forty-eight percent of gross domestic product. 5

China has the potential to play a particularly influential role in the global deployment of the Internet of Things. By 2020, there will be over 30 billion connected devices worldwide. 6 Already, China has more cellular device-to-device connections than any other country. 7 The overall market for the IoT in China will rise to $361 billion in 2020. 8 Though the majority of IoT device usage over the near-term will likely be by business and government, the next wave of IoT adoption will feature small business and consumers. Connected devices will be part of everyday life for many Chinese and even shape interpersonal communication through platforms like WeChat. Importantly, many IoT devices will also be manufactured in China.

**B. The digital economy is essential to China’s economic rebalancing**

China’s rebalancing aims to generate growth that is faster, more sustainable and inclusive. Doing so will require increasing domestic consumer consumption, innovation, and the number of people and businesses participating in the formal economy. The achievement of growth that is consumer-led, innovative, and inclusive demands a central role for the digital economy.

Consumption growth is linked to invigoration of services, which can be more easily delivered and accessed by digital channels. Innovation, meanwhile, grows with connectivity, which is a core trait of digital platforms. Digital is also a powerful driver of inclusion – for both individuals and SMEs.

McKinsey estimates the Internet will contribute up to twenty-two percent of China’s productivity growth by 2025. 9 In sum, the manner in which China leverages the digital economy will be a key determinant of future growth and development.
C. SMEs will be key digital actors

Since SMEs contribute about sixty percent of China’s GDP, their participation in the digital economy is essential. Other countries similarly depend on SMEs. For example, in the US, among high patenting technology firms, SMEs produce sixteen times more patents per employee than large enterprises. The “German Mittelstand” companies (Germany’s SME segment) are some of the most innovative in Europe, with fifty-four percent of them launching an innovation onto the market between 2008 and 2010.

For SMEs, embracing digital technology brings three key benefits:

- First, it enables access to more markets. This is critical in a world where more Chinese are shopping online and over 360 million shoppers engage in international e-commerce. Already, over 10 million SMEs around the world use Alibaba and over 50 million are on Facebook.

- Second, cloud computing now provides access to sophisticated technologies – storage, processing, connectivity, and, increasingly, artificial intelligence (AI) tools – at decreasing costs.

- Third, it enables greater personalization of products and services, a capability that will only grow in importance. While the impact of digital platforms on China’s SMEs and broader real economy has been largely positive, it is also creating new competitive pressures, particularly for micro businesses who sell commoditized goods. Even the smallest of businesses are now incentivized to sell more customized services to gain advantage over competitors large and small.

The extent to which China’s economic and innovation potential is realized will be heavily influenced by how quickly – and securely – its SMEs utilize these benefits.
II. NEW TECHNOLOGIES BRING NEW VULNERABILITIES

Though the potential benefits of digital transformation are clear, there is growing concern over the implications for the safety and security of data and personal information.

A. Individuals and SMEs are especially at risk

China’s individuals and SMEs generally lack the knowledge and resources to properly manage the accompanying risks of digital technology. As such, they can become weak links, negatively impacting not just themselves, but also the broader networks and supply chains of which they are often a part.

Such vulnerabilities are already causing substantial real-world harm. In 2014 and 2015, 900 million identities were exposed through hacks. Small businesses are no less safe. Nearly half the cyberattacks worldwide in 2015 were against businesses with fewer than 250 workers.

Digital threats often result from human mistakes. Business email fraud is a perfect example. This method of attack relies on the fact that customers and suppliers often communicate by e-mail. Hackers can exploit this by posing as a supplier and asking for payment of an invoice or the transfer of a funds to a new account.

- SMEs in the U.K. lose more than eleven billion dollars from invoice fraud every year, amounting to almost two thousand dollars per SME. Of 1,000 U.K businesses surveyed, nearly half have received a fraudulent or suspicious invoice in the last year.

- A major Austrian aerospace parts maker recently lost over forty-two million dollars in a business email fraud incident.

Chinese citizens have also been targeted:

- The Banking Regulatory Commission (CBRC) recently criticized several financial institutions for allowing their employees to sell personal information without corporate oversight.

- PBOC Deputy Governor Fan Yifei has highlighted telecom fraud as a growing source of identity theft, citing the need for a more coordinated government response.
B. The Internet of Things presents unique challenges

IoT devices present multiple risks – to security of data and personal information - over and above what is traditionally seen with desktop and laptop computers. Given China’s ability to play a prominent role in the future of the Internet of Things, it should pay close attention to both the risks and benefits of the industry.

Much of the value of connected devices will derive from analyzing the data they produce. The amount of IoT-related data will be staggering. A smart home can produce up to one gigabyte of data a week, while a connected car will produce up to twenty-five gigabytes an hour. A typical wind farm may generate 150,000 data points per second.

The IoT does not just create data, it also introduces untold numbers of entry points that can enable unauthorized access to, or control of connected devices. Just ten years ago, a typical large enterprise had about 50,000 endpoints in the form of devices, such as computers and point-of-sale terminals, on a network. By 2020, networks with tens of millions of endpoints will be the norm.

All this means more sensitive information will be vulnerable through more entry points. In addition, new infrastructure is needed to handle all the Internet traffic from the IoT. These new networks are not readily understood by all businesses and consumers and not always compatible with one another. Complicating matters further, securing IoT devices is more challenging than securing a home computer. And, especially with inexpensive devices, it is not always easy to update the software or apply a patch after the device has been sold.

Even though the Internet of Things is still in its infancy, we have already seen various examples of the security threats it can introduce, both to individuals and the overall ecosystem.

**IoT Risk of Serious Physical Harm**

Security researchers have shown that everything from connected cars to smart healthcare devices can be hacked. Through a variety of experiments, researchers have proven their ability to disable the transmission, engines, and brakes of Internet-abled automobiles, including in one instance where the car was driving on the highway. This has been done with multiple different vehicle types, reinforcing the broad-based and serious nature of the threat. Similarly, medical devices like pacemakers and drug-infusion pumps have been successfully compromised, demonstrating that connected devices can pose potentially fatal risks.
IoT Risk to Overall Ecosystem

As connected devices proliferate, they will present broader ecosystem risks, such as distributed denial of service (DDoS) attacks.

- In 2013, a massive DDoS attack took down China’s .cn country code top level domain for several hours. 25

- In the first half of 2016, there were almost 125,000 DDOS attacks a week 26, and in 2016, hackers conducted a major attack against Domain Service Name provider Dyn by using thousands of compromised connected devices to cripple the company’s servers. One of the largest DDoS attacks in history - almost twice as powerful as any before - it led to major sites like Twitter, Netflix, GitHub and Spotify experiencing service interruptions or going offline altogether for several hours. 27 The hackers were able to compromise the IoT devices mainly because the default passwords were not reset by the device users. 28

The total cost of breaches through digitization of consumers and businesses will reach $2.1 trillion by 2019 [Figure 2]

Figure 2: Internet of Things by the Numbers

Source: Juniper research, 2015; eMarketer, 2016; TSG, 2016
III. A VIBRANT DIGITAL ECONOMY NEEDS A COMPREHENSIVE AND MULTI-TIERED SAFETY AND SECURITY FRAMEWORK

China’s Standing Committee of the National People’s Congress promulgated a new Cybersecurity Law that is set to go into effect June 1, 2017. This law raises important safety and security-related issues in support of the development of China’s digital economy.

However, more remains to be done to protect individuals and SMEs so they can engage in, and fully trust the digital economy. The digital economy will not prosper without strong public trust.

Security efforts in the past have tended to emphasize detection and response. This time it’s different. Detection and Response are not enough. In today’s digital age, what is needed are more efforts at Protection. To strengthen consumer confidence in its next phase of growth, China should include a greater focus on Protection-enhancing tools, programs, and processes. To do so, Mastercard strongly recommends including more detailed guidance in four areas:

1. Standards for digital identity authentication;
2. Standards for data security;
3. Consumer awareness-raising; and

FOUR KEY PILLARS TO OPERATIONALIZE CYBERSECURITY

A. Digital identity authentication standards

If the digital economy is a primary driver of the economic rebalancing, then identity is fundamental to a successful digital economy itself. Proof of identity enables access to most business and government services. The number of identity-dependent transactions will only increase with the digital economy and growing connectivity between entities with no previous relationship, such as in cross-border transactions. Easy-to-use digital identity solutions also enhance consumer experiences, thereby driving greater adoption of digital products and services.
But identity is not just about seamless access to services, it is also about information security. Stolen identities are a major conduit for cyber fraud. In the U.S., compromised identities have represented the majority of entry points for major breaches over the past six years. Existing methods of managing identities are proving inadequate for the digital economy. A secure, easy-to-use digital identity credential is needed.

In addition to facilitating broader use of digital identities, China should embrace standards for authentication of such identities – for both individuals and devices. Strong authentication, like the use of a fingerprint or facial recognition, to even more basic steps like the confirmation of a one-time code, could have prevented almost 63% of the cyber intrusions carried out in the U.S. in 2015. Secure authentication is at the core of sound cybersecurity policy.

1. Authenticating individuals with biometrics

China’s cybersecurity policy would benefit from promoting secure and simple authentication solutions. These solutions should be meaningful, but also simple to use. Since biometrics enable the consumer to confirm they are genuine without having to remember a complicated password, they hide the complexity from the consumer and bridge the gap between convenience and security.

Wherever possible, we recommend two-factor authentication, which adds a second level of authentication to an account log-in and requires the user to have two out of the following three types of credentials before being able to access an account:

- Something you know, such as a personal identification number (PIN), password or a pattern
- Something you have, such as an ATM card, phone, or fob
- Something you are, such as a biometric like a fingerprint or voice print

In promoting strong authentication, China should encourage the adoption of open-source standards like the Fast Identity Online (FIDO) Alliance for consumer applications and Kerberos for enterprise applications. These standards use industry-standard public key cryptography and drive continuous and secure authentication across many devices. FIDO specifications, for example, enable mobile platforms to deliver multifactor authentication. Microsoft’s Windows 10 and multiple global financial institutions have adopted FIDO for consumer banking.
C. SMEs will be key digital actors

(germany's SME segment) are some of the most innovative in europe, with fifty-four technological innovations to enhance security protections. technology companies are platforms to deliver multifactor authentication. Microsoft's Windows 10 and multiple have been breached in 2016. 45 With the rise of IoT devices, these risks will only grow over

V. SECURING SMEs IS ESSENTIAL TO INNOVATION AND

Article 21 of China's Cybersecurity Law acknowledges the importance of a tiered vulnerabilities. Such an inventory of sensitive assets and information must be kept.

SMEs should first identity relevant databases, systems, substantial, as in healthcare applications, then it is recommended to put two-factor incorporate them into their overall cybersecurity efforts.

B. Data security standards

China should adopt data security standards that ensure IoT data is protected with, for example encryption or a token, no matter where the data is. Industry groups and governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 32 Strong data security tied to device identity authentication will ensure that data is encrypted and authentic, and that communications are secure.

Data security is also heavily dependent on the software and applications that manage IoT devices. In most of the known IoT incidents, the security weakness that were exploited were at the application layer. Therefore, China's cybersecurity strategy should also speak to the need for secure IoT applications and the requirement that IoT devices automatically receive software updates, including security patches. 33

Case Study: Biometric-Based Authentication

Our next generation solution, Mastercard Identity Check Mobile is a Mastercard-hosted solution designed to accommodate present (fingerprint and face) and future biometric methods of authentication across multiple devices. With Mastercard Identity Check Mobile, financial institutions do not have to burden their customers with multiple authentication methods. It also eliminates the need to create and remember static passwords. It provides a safer, simple, and consistent consumer experience—now and in the future—and is helping issuing banks improve operational efficiencies.

2. Authenticating devices using device IDs

Just as you need to know which humans you’re dealing with on the internet, you need to be confident of what device you’re communicating with. Given the impending ubiquity of consumer IoT devices, it is imperative that devices are also authenticated. This can be done using public-key cryptography to exchange public and private keys between the user’s registered device and a valid authentication platform. The combination of consumer biometric validation, device identification and device cryptography provides the enhanced security of multi-factor authentication that is becoming the global standard. For sensitive IoT device applications such as healthcare, two factor authentication should be used.

B. Data security standards

China should adopt data security standards that ensure IoT data is protected with, for example encryption or a token, no matter where the data is. Industry groups and governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 32 Strong data security tied to device identity authentication will ensure that data is encrypted and authentic, and that communications are secure.

Data security is also heavily dependent on the software and applications that manage IoT devices. In most of the known IoT incidents, the security weakness that were exploited were at the application layer. Therefore, China's cybersecurity strategy should also speak to the need for secure IoT applications and the requirement that IoT devices automatically receive software updates, including security patches. 33
As Article 15 of China’s Cybersecurity Law properly indicates, security standards should be informed by industry input. Examples of industry consortia addressing common concerns of security and interoperability include the Industrial Internet Consortium (IIC), the AllSeen Alliance, and the Open Interconnect Consortium (OIC). AllSeen and the OIC focus on standards for the IoT software layer, while the IIC promotes secure industrial IoT applications.

The Payment Card Industry (PCI) Council, as the body responsible for setting minimum security standards around the world for payment card security, is an excellent model for industry consortia.

Case Study: Industry Consortium Driving Global Standards
In order to harmonize and simplify compliance obligations at the merchant level, Mastercard and the other major payment brands mandate, on a global level, compliance with the Payment Card Industry Data Security Standard (PCI DSS) to ensure all merchants adhere to minimum security requirements in a more user-friendly fashion. Making security easier for merchants is one of the biggest differences PCI has made. Prior to the formation of the PCI Council, each payment brand had its own security framework and its own assessment process.

The primary purpose of PCI DSS is to reduce the risk of payment card data loss by preventing, detecting, and reacting to potential breaches or hacks that could lead to an account data compromise (ADC) event. With requirements for merchants, service providers, software developers, manufacturers of applications and devices used in payment transactions, the PCI SSC has now published nine security standards, 50+ guidance documents and essential tools needed for implementation of the standards, such as assessment and scanning qualifications, self-assessment questionnaires, training and education and product certification programs.

The goal of the PCI DSS is to protect payment card data from criminal threats and to minimize data breach risk to merchants of all sizes. The PCI DSS is based on 10 years of global industry and vendor input to create a stable technology standard that is often referenced outside of payments as a leading security standard.
IoT standards should drive ‘Security by Design’: China’s cybersecurity policy would gain by designating the above data security and authentication principles as necessary elements of pre-market IoT device design. In this way, security will not be an afterthought, but rather part of the product itself. As detailed earlier in this paper, design weaknesses in IoT devices, including discoverable default passwords and unalterable hardwired credentials, have already allowed attackers to cause significant harm. The goal is to build security into IoT devices in the same way that safety features, such as seat belts and air bags, have been engineered into automobiles.

**Case Study: Importance of ‘Security by Design’ for Widely Used Technology**

The automobile became widely available in the United States in 1908. However, it was not until the mid-1960s that a serious and coordinated effort to improve auto safety began. The car had become central to American life – like IoT devices will soon be – but large, and fixable, safety gaps existed for those intervening fifty years. Fixes included simple measures like seat belts, speed limits, and air bags. A period which saw tens of thousands of serious injuries and even deaths that could have been prevented. In 1973, the year before speed limits and seat belts began to be more broadly enforced, the U.S. saw 26 fatalities per 100,000 population. In 2015, when there were significantly more cars on the road, that figure had come down to 11.  

**C. Consumer awareness-raising**

Human behavior can often be the deciding factor in securing data or personal information. Virtually every international, regional, and country-level framework, including that from the United Nations-initiated Group of Government Experts (GGE), European Union, Germany, United States, and Canada, emphasizes the importance of raising public awareness. For example, Canada’s recently released “Renewed Approach to Cyber Security’ highlights as one of its three main actions areas the need to build resilience by creating “greater public awareness of cyber threats and how individual Canadians and businesses can protect themselves.”

In addition to supporting public awareness initiatives, China’s cybersecurity framework should embrace a standardized digital product label and rating system. This would empower consumers to buy more secure devices, there creating economic incentive for IoT device makers to add security protections.
C. Consumer awareness-raising

Public awareness campaigns: Until a standard label and rating system is developed, China should pursue aggressive public awareness initiatives with simple and concrete recommendations. The goals of raising public awareness should be to: (1) encourage consumers to change default passwords and select appropriate security preferences; and (2) ensure that consumers understand the security implications of using connected devices.

Security risk labels and ratings for devices: The ultimate solution is to design a system with two elements: (1) a standard label that conveys information on the product’s cybersecurity-related risks and how easily the product can be secured; and (2) a rating system to reflect each product’s security level, based on independent third-party assessments. A system of tiered ratings is preferred as it would motivate IoT makers to do more than the bare minimum. The system that rates appliances based on energy usage could be a template as could the system behind food packaging and nutrition labels.

D. Capacity-building for businesses

Workforce education: As the digital economy grows, more jobs will demand a minimum level of cybersecurity knowledge. China will need to provide on-the-job training for its current workforce and increase the pipeline of skilled cybersecurity professionals. Chinese government and business should work together to enhance university-level cybersecurity programs and scholarships, while also incorporating basic cybersecurity know-how into primary and secondary school curricula. Everyone from young students to senior executives and government officials should possess a baseline level of cybersecurity knowledge.

China holds a National Cyber Security Awareness Week every year and has launched a RMB300mn cybersecurity fund to provide financial assistance to experts and teachers who specialize in cybersecurity.

The U.S. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework identifies several categories of cybersecurity work, including more than 30 specialty areas and 50 work roles. This can be used by China to undertake a more detailed evaluation of its current cybersecurity workforce and potential gaps.
**New security solutions:** Businesses should consider augmenting human capability with advanced analytics tools. No matter how sophisticated, every fraudster leaves a data trail. Machine learning algorithms aggregate this data into signals that are predictive of fraud. As the name implies, these algorithms learn over time, helping to stay one step ahead of criminals. Such artificial intelligence (AI) applications can be used against behavioral data as well to better protect consumers without introducing more friction into their lives. AI-driven solutions can also help address the growing threat from organized, large-scale cyberattacks. Recent advances are making these technologies less complex to use. This means that businesses of all sizes can leverage the power of AI to drive stronger safety and security.

Article 18 of China’s Cybersecurity Law encourages the development and use of technological innovations to enhance security protections. Technology companies are essential to helping realize this vision.
IV. THE IMPORTANCE OF HARMONIZING WITH BASELINE GLOBAL NORMS

The private sector will be a strong partner to help China achieve progress in the four areas detailed above, provided a predictable business environment exists. Stronger public-private partnership can be achieved by harmonizing the cybersecurity framework to three baseline global norms: (1) Adherence to international standards; (2) Global interoperability; and (3) Multi-stakeholder collaboration.

A. Adherence to international standards

Hackers do not respect borders. In view of this, aligning national cyber security requirements with international standards is the best way to ensure a safe & secure digital ecosystem. In the absence of harmonization, the international community will tend toward entrenched and less secure technologies, inevitably impairing cyber security.

Article 7 in China’s Cybersecurity Law acknowledges the importance of international cooperation. It would benefit from greater detail on the relevance of global norms. It is recommended that China adapt and help shape existing and developing global frameworks, enhancing them for the betterment of all. There are two advantages to this approach. First, driving change within an existing system is easier than establishing a new system. Second, there is ample opportunity to achieve global leadership in the context of current frameworks, which can incorporate and enhance new input, while preserving the benefits of prior work.

The Chinese government is working to make the Internet of Things a key part of its economy. It is building a national plan for the IoT industry and has invested substantial sums in IoT projects. China is also developing an IoT standards association and advocating for its own approach to safety and security more broadly in various bilateral, regional, and global fora. We commend China’s active participation in the International Telecommunications Union (ITU) and the UN-initiated GGE. The GGE 2015 report highlights the need to “[f]acilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders.”

China should take a more proactive leadership role in such cross-border cooperation and help shape international harmonization of security standards. Both the European Union Network and Information Security Directive (NIS) and the joint EU-China effort
on the IoT, as well as other approaches, highlight the importance of participating in the development of, and adherence to global security standards.

Section 5 of the EU-China IoT Advisory Group white paper encourages Europe and China to support “the development of international standards for the IoT business layer, in the activities of international standardization organizations such as OneM2M, ETSI, CEN/ ISO, IEEE, IETF and ITU-T.”

Further, the EU NIS Directive states that “[t]o ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level.”

B. Global interoperability

Forty percent of all the potential value associated with the Internet of Things requires interoperability between IoT systems. Lack of interoperability is an obstacle not just to security, but also to user experience, since without interoperability every smart device in your home, for example, will need a separate app. Interoperability lets data move across all IoT layers – whether hardware, software, or applications - and ensure that solutions work across devices.

The European Commission’s Digital Single Market Strategy underscores the need to promote interoperability for the IoT industry to meet its potential. Similarly, the joint white paper by the EU-China IoT Advisory Group rightly emphasizes interoperability and standards cooperation, stating: “the IoT requires standards to enable horizontal platforms that are communicable, operable, and programmable across devices, regardless of make, model, manufacturer, or industry. The vision is that connectivity between people, processes, and things works no matter what device, software, interface and data are used.”

Case Study: Importance of Interoperability

In the early years of the Information Technology industry, sending an e-mail using one corporation’s application to another user in a different institution using another vendor’s application was not easy. Once the Internet was widely embraced, it became easy to send an e-mail between companies. This was because everyone was using the same standards, including open source implementations of key protocols. Rather than developing their own proprietary networks, institutions collaborated on developing the common Internet architecture – and Internet-based applications like e-mail and the Web.
Much of the success of the Internet is due to the international organizations that oversaw the development of standards and made available open source implementations of their software releases, thus encouraging open, collaborative innovation. The lesson was that you need to get the architecture right, agree on open standards, develop open source platforms and set up governance processes embraced by all.

Like the Internet in the early 1990s, the Internet of Things is at the early stages. China and the world must do with digital and cybersecurity what was done for the Internet and connectivity.

C. Multi-stakeholder collaboration

The total cost of cybercrime worldwide in 2015 was $500 billion, and the cyberattacks that cause the most damage are those twenty percent that are of an unknown variety. [Figure 3] This insight alone shows the essential nature of cross-sector knowledge-sharing. Indeed, progress toward a more secure cyberspace is only possible with a multi-stakeholder approach.

Figure 3: Global Cost and Unpredictable Nature of Cyberthreats

The threat landscape and security response

- Total cost of cybercrime worldwide
- 80% of attacks are of a known variety - the other 20% cause the most damage

Source: Forbes, 2016
Source: IBM, 2016
Without a coordinated response, cybercriminals will continue to innovate and find vulnerabilities in international security structures. Recognizing this, the European Union's Network and Information Security Directive requires collaboration on significant cybersecurity incidents and greater harmonization of member state laws and capabilities. The UN GGE, of which China is an active participant, has also noted that the private sector and civil society should contribute to the development of cybersecurity norms. 44
V. SECURING SMEs IS ESSENTIAL TO INNOVATION AND LONG-TERM GROWTH

Just as many individuals do not fully understand the security implications of using connected devices, many SMEs may not realize they, too, are vulnerable. Forty-three percent of cyberattacks globally are directed at SMEs, and fifty percent of small business have been breached in 2016. With the rise of IoT devices, these risks will only grow over time. SMEs face an exploding number and variety of cyber threats with limited resources and capabilities, making them a weak link in the global cybersecurity chain. Since cybersecurity is only as strong as its weakest link, securing SMEs must be a priority.

Article 21 of China’s Cybersecurity Law acknowledges the importance of a tiered approach, but would benefit from separate, detailed guidance for SMEs. The European Union’s Agency for Network and Information Security (ENISA) has released information security standards specifically for SMEs. Similarly Canada, the United States, and Germany offer advisory documents directed at SMEs. These reference standards and implementation guidelines emphasize that the authentication and education initiatives relevant for individuals are also important for small businesses. These guidelines also highlight the need for SMEs to make efficient use of limited resources by adopting a layered approach. Since all threats are not the same and SMEs do not have unlimited resources, this type of strategy is essential.

Core Elements of Layered Implementation Framework for SMEs

Adopt risk-based approach: SMEs should first identify relevant databases, systems, applications, and devices, and assess the risk of each. What constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Such an inventory of sensitive assets and information must be kept up-to-date. Equipped with this knowledge, SMEs can then focus their scarce resources where the risk to sensitive information is the greatest.

Apply ‘security by design’ system: Instead of imposing security as an afterthought, SMEs should build appropriate tools and protocols into their organization, products, and services as part of the planning process, including by choosing safer options as the default settings for IoT devices and software applications. If the risks are substantial, as in healthcare applications, then it is recommended to put two-factor

Ensuring Security and Prosperity in the Digital Age
In promoting strong authentication, China should encourage the adoption of FIDO specifications, for example, enable mobile authentication across many devices. This can be done using public-key cryptography to exchange public and private keys. In this regard, China should explore professional training programs for small business Information Security Officers.

**Encourage culture of security:** Staff training is critical. Fighting business email fraud, for example, requires email security software but also employees that know how to identify signs of fraud in email. SMEs should consider designating an Information Security Officer to ensure organizational ownership of information security and data protection functions. In this regard, China should explore professional training programs for small business Information Security Officers.
VI. SUMMARY

China’s new Cybersecurity Law raises important safety and security-related issues that will be relevant to the development of its digital economy. The Law would benefit from more detailed guidance designed to drive action in four areas, particularly as they relate to individuals and SMEs:

1. Standards for digital identity authentication;
2. Standards for data security;
3. Consumer awareness-raising; and

The private sector can be incentivized to meaningfully partner in these areas, provided a predictable business environment exists. This can be achieved by aligning China’s cybersecurity framework with three critical global norms: (1) Adherence to international standards; (2) Global interoperability; and (3) Multi-stakeholder collaboration.
Since SMEs contribute about sixty percent of China’s GDP, their participation in the
c. SMEs will be key digital actors heavily influenced by how quickly – and securely – its SMEs utilize these benefits.

Wherever possible, we recommend two-factor authentication, which adds a second

China’s cybersecurity policy would benefit from promoting secure and simple

security. Stolen identities are a major conduit for cyber fraud. In the U.S., compromised

Strong authentication, like the use of a fingerprint or facial recognition, to even more

V. SECURING SMEs IS ESSENTIAL TO INNOVATION AND

resources where the risk to sensitive information is the greatest. 47

SMEs should first identity relevant databases, systems,

education initiatives relevant for individuals are also important for small businesses.

will only grow in importance. While the impact of digital platforms on China’s

tools – at decreasing costs.

incorporate them into their overall cybersecurity efforts.

combination of consumer biometric validation, device identification and device

ubiquity of consumer IoT devices, it is imperative that devices are also authenticated.

Just as you need to know which humans you’re dealing with on the Internet, you need

to device identity authentication will ensure that data is encrypted and authentic, and

International Telecommunications Union (ITU) and the UN-initiated GGE. The GGE

bilateral, regional, and global fora. We commend China's active participation in the

advocating for its own approach to safety and security more broadly in various

sums in IoT projects.  China is also developing an IoT standards association and

Standards; (2) Global interoperability; and (3) Multi-stakeholder collaboration.

The digital economy will not prosper without

The People's Bank of China (PBOC) captures the seriousness of the threat. In September 2016, they published a report on a "cyberattack against a top five Chinese bank in the 2016 second quarter.


20    “Prevent Invoice Fraud and Protect Your Business.” The Telegraph, May 2016

21    Gigaom article, July 2014

22    Quartz article, 2016

23    “Scaling Data Science for Industrial IoT.” O’Reilly Report, 2017

24    “How the Internet of Things Got Hacked.” WIRED, 2015

25    Center for Strategic and International Studies Report

26    Tripwire article

27    Cybersecurity Commission Report, United States

28    ABC News article, 2016


30    Cybersecurity Commission Report, United States


33    “Combating IoT Cyber Threats, IBM DeveloperWorks best practices

34    National Highway Traffic Safety Administration data, United States


36    General Office of Hubei Provincial People’s Government

37    Global Times article

38    2015 Consensus Report, UN Group of Governmental Experts

39    EU-China IoT Advisory Group white paper

SOURCES

1    “China’s Transformative Technologies.” McKinsey & Co article, August 2015

2    CNNIC Report, 2017

3    “Three Great Forces Changing China’s Consumer Market.” World Economic Forum article, January 2016


5    AliResearch and Boston Consulting Group Study

6    Gartner and Juniper Research

7    “How China is Scaling the Internet of Things.” GSMA Report, July 2015


10   International Finance Corporation Report, October 2012


12   Germany’s Federal Ministry of Economics and Technology


14   Ibid

15   Nilson, Mastercard data

16   Symantec Report, 2016

17   “Prevent Invoice Fraud and Protect Your Business.” The Telegraph, May 2016

18   “Could You Be Sending Your Firm’s Cash to Fraudsters?” BBC, September 2016


20   Ibid

21   Gigaom article, July 2014

22   Quartz article, 2016

23   “Scaling Data Science for Industrial IoT.” O’Reilly Report, 2017

24   “How the Internet of Things Got Hacked.” WIRED, 2015

25   Center for Strategic and International Studies Report

26   Tripwire article

27   Cybersecurity Commission Report, United States

28   ABC News article, 2016


30   Cybersecurity Commission Report, United States


33   “Combating IoT Cyber Threats, IBM DeveloperWorks best practices

34   National Highway Traffic Safety Administration data, United States


36   General Office of Hubei Provincial People’s Government

37   Global Times article

38   2015 Consensus Report, UN Group of Governmental Experts

39   EU-China IoT Advisory Group white paper

Ensuring Security and Prosperity in the Digital Age 22
C. SMEs will be key digital actors

For SMEs, embracing digital technology brings three key benefits:

1. Greater productivity and efficiency
2. Enhanced customer experience
3. Improved decision-making

Furthermore, cybersecurity is critical to helping realize this vision. SMEs are especially at risk from organized, large-scale cyberattacks. Recent advances are making these attacks more sophisticated and targeted.

AI-driven solutions can also help address the growing threat of cybercrime. These technologies can improve detection and response capabilities, helping to prevent and mitigate cyber threats.

Wherever possible, we recommend two-factor authentication, which adds a second layer of security. This can be done using public-key cryptography to exchange public and private keys securely. Cryptography provides the enhanced security of multi-factor authentication that is essential for protecting sensitive data.

Data security is also heavily dependent on the software and applications that manage critical information. Since all threats are not the same, it is recommended that China adapt and help shape existing and developing global frameworks. The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards.

B. Data security standards

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards.

C. Multi-stakeholder collaboration

This can be done using public-key cryptography to exchange public and private keys securely. Cryptography provides the enhanced security of multi-factor authentication that is essential for protecting sensitive data.

Data security is also heavily dependent on the software and applications that manage critical information. Since all threats are not the same, it is recommended that China adapt and help shape existing and developing global frameworks. The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards.

B. Data security standards

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected. 33

The Chinese government is working to make the Internet of Things a key part of its national strategy, and they should adopt data security standards that ensure IoT data is protected with industry standards. 32 Strong data security tied to governmental frameworks alike agree that whether the data is being generated, transferred, stored, or processed, it needs to be protected.