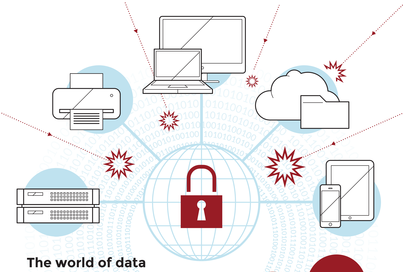
WHERE TRUST BEGINS

PROTECTING THE CONNECTED ECOSYSTEM

The connected computing reality has changed our lifestyles while creating new needs and expectations. While constant Internet access offers many benefits, including instant access to data and connectivity among many kinds of devices, there are downsides.



The world of data

According to IDC, in 2013 there were almost as many bits of data in the Digital Universe as known stars in the physical universe, and by the year 2020 the Digital Universe is expected to reach

44 Zb

(ten times the size of 2013)

Total number of devices (bn)

The Internet of Things (IoT) is growing over three times as fast as traditional IT, and by 2020 will nearly equal all other IT spending. Research conducted by Cisco Systems indicates as many as 50 billion installed connected things by 2020.

Contributing significantly to the vast streams of data created today are increasing numbers and kinds of devices. According to estimates, the number of mobile phones will exceed the world population in 2014.

Computers in use will reach the 2 billion mark next year.

85% Most of that data (about 2/3) is created by the individual consumer, but 85% of all the content falls within the responsibility of the enterprises acting as owners/custodians of:

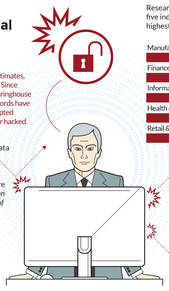
- personal data
- payment processing records
- proprietary corporate data
- medical records
- authentication credentials
- financial & banking data

Security is mission critical

50%

About half of the data, IDC estimates, is currently UNPROTECTED. Since 2005, the Privacy Rights Clearinghouse reports that 536,508,478 records have been breached from unencrypted drives that were lost, stolen or hacked.

Consider the Heartbleed vulnerability, the massive data breach at Target and the recently reported eBay phishing scams. It turns out almost half of the attacks are classified as *opportunistic - an attack that takes advantage of existing vulnerabilities or weaknesses without any specific motivation*. Furthermore, IBM ranks the human factor as the most prevalent element contributing to vulnerability of an average organization:



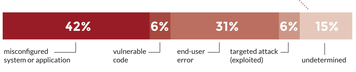
Research from IBM identified five industries with the highest share of attacks:

- Manufacturing **26.5%**
- Finance & Insurance **20.9%**
- Information & Communication **18.7%**
- Health & Social Services **7.3%**
- Retail & Wholesale **6.6%**

During a period of 12 months, any IBM-monitored client on a weekly basis suffered on average

200 malicious attacks

1.7 security incidents



The costs (US$ million)

IBM and Ponemon Institute research points to the significant increase in average total organizational cost of data breaches over the period of one year:

The big chunk of it relates to the average "lost business" cost

Three specific factors can significantly reduce the average cost per lost record:

*Chief Information Security Officer

Trusted Computing: A Foundation of Trust for Devices and Transactions

The Trusted Computing Group (TCG) enables a secure foundation for all types of computing: its open, vendor-neutral industry specifications include the TPM for establishing a root of trust, as well as software interface specifications across multiple platforms and operating environments that improve the security of data, devices and networks.

In a 2012 report, Aberdeen Group made a case for using TPM as a hardware root of trust:

- Trusted Platform Module
- No hardware root of trust

Cost per endpoint (US$)

56

71

Security-related incidents

4

8

Cost avoidance (at an average cost of $520 per incident)

520

Data, devices and networks are insecure. The TPM provides embedded security including:

1/2 half the cost of a smart card

built-in authentication

1/3 one-third the cost of a token

Root of Trust (RoT)

RoT is hardware, firmware, and/or software that is inherently trusted to perform a vital security function.

As computing environments become more complex, more security functions will rely on Root of Trust (RoT). This will be the case not only in the original TPM target platforms of desktop and notebook deployments, but also in the mobile, virtual and cloud server environments, as well as the embedded computing space and IoT devices ranging from cars to factories to appliances and more.

TPM Mobile
TPM Mobile offers a hardware root of trust in the device for secure transaction, secure storage of keys and certificates and integrity assurance

Self-encrypting drive
SED solutions based on TCG specifications enable integrated encryption and access control within the protected hardware of the drive

Some of the TPM applications devised and endorsed by the members of TCG

Cloud Computing
Trusted Computing concepts allow cloud users to establish trust, exchange information about the platforms they use and assure compliance to agreed policies

Trusted Network Connect
TNC specs enable endpoint posture assessment, intelligent access control and security automation for compliance with network/enterprise security policies

Sharing a common TCG approach

With that in mind, TCG offers a broad foundation of support for now and the future:

Sharing a common TCG specification would be more economical than fragmented solutions, reducing the cost of goods for vendors, developers, and suppliers and cost of ownership for users of technology. Federal and international legislation mandate the use of strong security measures to protect information, as shown by the 2013 FTC ruling, which imposed clear guidelines after a "failure to take reasonable steps to secure the software it developed placed sensitive information about millions of consumers at risk".

The evolution of trusted computing and TCG:

1. **Pervasive deployment of TCG technology**
   Not just in PCs, but in a wide range of devices, including mobile and the cloud
2. **Creation of the trusted platform**
   BIOS, TXT, operating systems, storage, secure I/O
3. **Expand trusted computing to the more complex systems**
   Servers, virtualization, networking infrastructure
4. **Connect networks and systems**
   Including the Internet of Things (IoT) and the Cloud
5. **Build resilient security**
   Create a robust, standards-based ecosystem for proactive security

JOIN the quest to develop and promote trusted computing technologies, and become a part of the global circle of trust.

SOURCES: Aberdeen Group, Bloomberg, Cisco Systems, ComputerWorld, Ericsson, Federal Trade Commission, Forbes, IBM, IDC, Ponemon Institute, Trusted Computing Group, Verizon, Wall Street Journal

TRUSTED COMPUTING GROUP™