

A close-up photograph of the valve section of a brass instrument, showing two valves with silver-colored caps and the surrounding gold-colored tubing.

We make technology sound



Published 28 September 2010

Contact Person  
Erwin Selg – CTO Office

Address  
GFT Technologies AG  
Eilderhauptstraße 142  
70599 Stuttgart  
GERMANY  
T +49 711 62042-0  
F +49 711 62042-101

## Table of contents

1 IT security trends.....	3
2 CTO Comment Box.....	8
3 NewsWatch.....	9

The TechReport is published on a monthly basis and wants to inform a broad audience about the latest trends and developments of the IT industry. The intention of the TechReport is to make trends transparent and understandable within their context and give the readers impulses for their business. The content has been created with the utmost diligence. Therefore, we are not liable for any possible mistakes.

### **GFT Technologies AG**

Executive Board: Ulrich Dietz (CEO), Marika Lulay, Dr. Jochen Ruetz, Chairman of the Supervisory Board: Franz Niedermaier  
Commercial Register of the local court (Amtsgericht): Stuttgart, Register number: HRB 727178

Filderhauptstraße 142, 70599 Stuttgart, GERMANY  
T: +49 711 62042-0, F: +49 711 62042-101, M: ctio.office@gft.com

Copyright © 2010 GFT Technologies AG. All rights reserved.

## 1 IT security trends

IT security and compliance are proving an increasing challenge to companies operating in a networked world. IT security aims to protect from threats and hazards, as well as prevent damage and minimise risks.

### IT infrastructures are becoming increasingly complex

Early computer systems were not usually networked. To exchange information, dedicated data media and processes were needed. By contrast, modern systems have achieved high levels of connectivity. This has not only changed the way malware and other malicious attacks work. There has been a huge increase both in the number of ways infections attack systems and the methods used to access IT systems and data.

Today, the necessity of IT security is no longer questioned.

Businesses – employees, partners, subcontractors and clients – need to access information anytime, anywhere to secure a competitive edge. With an increasing number of companies outsourcing services, drawing on external services and calling on cloud computing services, the boundary between internal and external processes is become more blurred. Systems and processes have become so interwoven that it can be extremely difficult to pinpoint clearly local versus remote attacks, or even separate out internal and external employees. Classic static security measures cannot solve this problem, as the storage/process locations are no longer precisely defined. Thus, the only way to minimise risks is to oversee systems through overarching IT security management processes.

### IT security incidents are on the rise

After a difficult 2009, many analysts predicted a rise in global corporate IT spending. Various studies by malware analysts such as McAfee, Symantec, Kaspersky, large software houses (such as Microsoft, IBM) and even bodies like the German Federal Office for Information security, the German Federal Criminal Police Office and the German IT industry association BITKOM, have shown that cybercrime still poses a significant threat to businesses and it is becoming more and more professional.

Cybercrime, industrial espionage via the internet and social network threats are booming.

As in the past, cybercrime has continued to develop and has been growing steadily in scope and maturity. Recent studies prove that companies are increasingly afraid of falling to virtual attacks. Part of this is definitely due to the fact that – apart from the well-known risks from script nerds, hackers and criminal entities – awareness of industrial espionage risks is also being taken more seriously. One example was the AURORA incident in January 2010 when it was revealed that more than 30 companies (including Google, Intel, Symantec and Adobe) had become victims of a carefully planned espionage attack.

In addition to this, incidents of identity theft and account hacking are also on the rise as the market for such data is becoming more and more lucrative for criminals. Apart from major online attacks, it is also important to note bank data theft in this context (e.g. CDs with listing names of tax evaders in Germany).

IT security reduces risks– from the design and software phase to implementation and operating of software.

### There will be no secure software

Although much progress has been made in recent years in integrating security issues into modelling and software implementation and although quality management awareness has risen, users and companies have no choice but to take their own steps to improve security. Despite tools like static or dynamic code analysis and ever-improving fuzzing tools, software is still vulnerable to weaknesses. The problem is that most modern software is so complex. Even testing procedures – specially embedded within the development process – or newer program languages such as Managed Code - are no guarantee that a program

will be secure and free from bugs. Despite this, IT security can do a lot to minimise risks – from the initial development process to software implementation and entire infrastructures and processes.

#### Gateways for malware have increased

**Classic perimeter protection is no longer sufficient for IT security.**

And because of this, software introduced to businesses is still a gateway to attack and will continue to be used as a trigger for malware. Malware used to spread through emails and data media, but now it is increasingly being distributed via websites and social networks. One of the preferred options is to misuse trusted websites by infiltrating foreign codes through XSS, XRSF and SQL injection techniques. Apart from exploiting the vulnerabilities of web browsers, attackers increasingly now use malfunctions in so-called plug-ins as they are often out-dated and companies fail to include them in patches and updates.

#### Multilayer and multilevel security

**The future lies in the application of multilayer and multilevel security.**

Another important aspect when it comes to IT Security is the fact that there is no universal product or method to protect system infrastructures and information. The key to success in protecting systems and data lies in multilayer and multilevel security measures. The term multilayer is used in this context as it involves examining security at different levels and not just relying on one product or procedure. Just as a fortress may have several ramparts, infrastructure must be protected by several procedures so that if one mechanism fails, the next one should succeed.

The term multilevel centres on the interaction between subjects and their access to objects. Integral to multilevel systems are the guidelines used to authorise subjects and classify objects, as well as the assignment of permitted methods and actions. A typical example of a modern solution that works along these lines is a cross domain system (CDS), which focuses on the exchange of data in computer networks.

#### Classic protection techniques

**Virus scanners and firewalls are not outdated, but they are no longer sufficient protection measures.**

Virus scanners (including spam and spyware scanners), firewalls and proxies are now the established way to offer basic protection to infrastructure and IT systems. However, they are only a small part of security concepts and more and more often they are proving insufficient. Virus scanners need actual malware signatures. As a consequence, it will always be a major problem managing and distributing such data. In the future, most providers of such products will become service providers, to enable real-time enquiries of their data. This fails to address the issues of data protection and internal corporate information, however. The problem with firewalls is that more and more attacks and data losses are occurring through legitimate connections, which firewalls are simply powerless to prevent. Content-aware proxies can be a solution in this respect.

#### Established enhanced protection mechanisms

##### Anomaly /attack identification systems

**HIDS and NIDS are not competing against each other, but complementing each other.**

In recent years there has been an increase in anomaly/attack identification systems. Intrusion detection systems (IDS) are worth mentioning in this context. These are passive systems that observe actions or communication flows.

There are host-based IDS (HIDS) and network-based IDS (NIDS). HIDS operate on the protection system itself, creating events whenever an anomaly is identified. "System integrity verifiers" are a subcategory of HIDS. They are able to identify system modifications by using checksums. NIDS act as a complement to HIDS in that they monitor network traffic. NIDS use sensors to help monitor a whole variety of connections to a variety of systems. Newer hybrid IDSs link up HIDS and NIDS, thus achieving a higher identification

rate. In addition to this, Hybrid IDSs offer a central management system for the sensors. Another IDS development relates to intrusion prevention systems (IPS). These automatically trigger countermeasures in the event of an attack. Honeypots are another approach to identify attacks. Honeypots activate network systems that do not offer real services, but only pretend to. Using honeypots is a fairly simple way to analyse attack patterns and attack behaviours. If whole networks of systems are imitated, then these systems are known as honeynets.

#### Application firewalls

A web application firewall (WAF) either operates as a fully independent system or as a server plug-in which uses rules to monitor communication with a service. Usually these are web services via HTTP protocol. In general, they can prevent general attack vectors like XSS, SWL injection or information disclosure. WAFs can be configured at a highly granular level to prevent further attacks. WAFs are an especially good choice when protecting existing web services, especially if it would be too much effort to modify an application to increase security or remove security leaks. WAFs protect web applications the same way that database firewalls protect access to databases. Database firewalls monitor database communication, and apart from identifying and preventing attacks (e.g. SQL injections) they can inhibit infiltration by database rootkits. Thanks to the increasing use of cloud computing and web services, in the future increasing use will be made of application firewalls and they are a useful complement to classic firewalls.

**Application layers are increasingly becoming the focal point of communication protection.**

#### Network access control systems

Due to today's high level of connectivity, it is of utmost importance to track who receives access rights to the corporate network. Sometimes also referred to as network admission control or network access protection (NAP) systems, network control systems (NAC) check if terminals comply with guidelines during authentication processes. Only after successful checks is a terminal granted access to the respective network segment. At the same time, the system identifies hardware, software, software versions (security patches and malware signatures) and the user identity.

**NAC/NAP systems control access to internal infrastructure and apply compliance requirements to the end-user system.**

#### New challenges for IT security

Many of the old, familiar problems still present a challenge to IT security – and now they have been joined by new ones.

#### Mobile computing

This does not just refer to the broader, complex nature of ubiquitous computing, and recent developments such as mobile computing – hand in hand with the management and protection of terminals (smart phones, web pads etc.). This is just the tip of the iceberg. Devices categories and software systems are expected to diversify in the future. To manage and keep systems secure, standards and uniform interfaces will be needed to cater to the complete range of possible devices. Mobile devices cannot be ignored when it comes to security, as they are just as capable of accessing and processing information as laptops and work station computers.

**Established security processes must be adapted to work with mobile devices.**

#### Virtualisation

Without a doubt, the trend towards systems virtualisation has many advantages. To handle this new type of environment, however, in-house security policies must be updated as new risks are joining the ranks of the established risks. First, systems are gaining a new, complex software layer (the virtualisation layer). Operating several systems on a single piece of hardware opens the door to new system vulnerabilities. Apart from the existing network system interfaces, attackers now have the possibility to exploit the software layer to

**Virtualisation has tremendous potential to cut costs.**

reach a virtual machine (VM) from another VM. This must be built into the risk analysis when systems are merged. Second, resource distribution between VMs has to be evaluated to prevent resource bottlenecks and interference with (or the breakdown of) important services. Further, it is important not to compromise existing network security levels. Most of the time, virtual switches from virtualisation suites do not offer the same security functionalities as real network components. As well as restructuring access management for administrators, it is necessary to update recovery management.

#### Cloud computing

**Risk analysis comes before cloud computing, covering the understanding of risks as well as a classification of data and processes.**

Not only does cloud computing offer new opportunities, it brings new risks that need to be taken into account. By outsourcing data to external service providers, companies no longer have to worry about data storage. However, this involves investing a huge amount of trust in the service provider. How can companies guarantee that the services will remain usable in the long run? Or that external service providers will handle hosted data responsibly? Data stored online does not have the same protection level as data within the in-house infrastructure – from a technical and legal point of view. Companies are delegating control over who receives access to data, where data is processed, and how. No one can be 100 per cent sure that data is fully protected, has not been manipulated or is being correctly deleted. In addition to this, the risk of becoming a victim of a cyber attack increases, even if the target of the attack was not the company. By pooling different types of data at cloud computing service providers, it becomes a tempting target for attackers.

These open questions need to be resolved by IT security experts. To minimise risks, the right technology needs to be put in place and certain prerequisites have to be fulfilled. Encryption is just one small part of the equation.

#### Social networks / communication platforms

**Internet social networks are an excellent source of information. DLP systems help to maintain control over company data.**

An increasing number of external social networks and communication platforms are being integrated into business and communication processes. The workflows and information processes involved must also be taken into account when designing security procedures.

It is thus necessary to create simple and granular control mechanisms capable of monitoring the stream of information and making all information inaccessible (e.g. no longer readable) when disconnected from specified locations or processes.

Data leakage protection/prevention (DLP) products can help in this respect. However, this promising new area of IT security is still wrestling with organisational problems. If these tools are to expand beyond “special” use, the IT security industry needs to develop even more sophisticated tools, plus procedures for improved automated classification of information and effective rights administration.

#### Security/awareness among employees

**Mere technology is not enough. Make sure that employees are not the weakest link in the security chain.**

Business risk can be prevented on more than the technical level. It is of the utmost importance that employees are aware of the risks and take responsibility for them. Companies need to provide strict communication guidelines for the publication and processing of information so that employees are protected against social engineering attacks. However, placing employees under too severe restrictions can also be counterproductive so instead they should be made aware of the risks. Data theft is often possible without active support from an internal employee. Not knowing about the risks or naïve attitudes often lead to an unwanted loss of corporate data. For this reason, it is important to train employees and make them aware of the risks not just of publishing information but also the nature of new security risks. The only way to ensure employees know what to do in an emergency is to practice procedures regularly. Create clear security

systems and make it possible for employees to ask for expert information and ask about procedures at any time, on any kind of issue.

#### Monitoring, patch management and incident management

To safeguard business operations, it is crucial to know the status of systems. Useful support comes in the shape of network and system monitoring solutions. To know what to do, weaknesses, bottlenecks, attacks and breakdowns have to be identified. One of the most important fundamentals of a secure infrastructure is to keep the system up to date and install patches aimed at minimising security risks as soon as possible. “Install and forget” systems are a great problem. Only with a properly defined patch management process and the help of patch management software can systems be kept up to date. In addition to this, infrastructure has to be audited on a regular basis. Here a vulnerability scanner is an indispensable part of vulnerability management. No infrastructure is immune to breakdowns, attacks or misuse. So it is essential for companies to be in a position to recover systems and services as quickly as possible after an incident and thus minimise the consequences. Companies thus need a clear security incident management plan to work in parallel with the classic incident management plan. Incident management systems (IMS) support companies in creating and adhering to emergency plans.

**Security is a cyclical process. Seamless monitoring and a clearly defined patch management minimises the risk of a security incident.**

#### IT security standards and compliance

IT security policies are the foundation of corporate IT security management. But corresponding processes and responsibilities are just as important as it is these that make sure policies can be maintained and updated. IT security never stands still; it is a process which needs constant adapting and updating!

Standards can help companies with the implementation of IT security policies and guarantee wide-ranging protection. These include:

- ITIL/ISO 20000 – IT Service Management
- ISO/IEC 2700x Series - Information Security Management System
- BSI IT-Basic protection – protection analysis
- ISO/IEC 15408 – Common Criteria
- OSSTMM – Security Testing

More recent laws and regulations (SOX, Basel II, HIPAA, PCI-DSS) oblige companies to implement these IT requirements. This also relates to IT security. Standards enable companies to fulfil requirements, and certificates provide proof of implementation. In future, security certificates will play an increasingly central role in business to business relationships, as they are the only way to guarantee that a client or business partner is implementing certain processes and mechanisms and has a certain level of IT security awareness.

#### Conclusion

IT security is not just a means to an end. It is about protecting assets and data – and thus, ultimately, the company itself. Although this article only gives a rough overview of the broader, more complex area of IT security, it perhaps demonstrates the scope and complexity of the issue. IT security cannot be marginalised within companies. It must be taken extremely seriously. IT security can by no means be considered a secondary activity. It must be given the priority it deserves, plus plenty of time. Continuous employee training is required to ensure staff remain focussed on the issue and thus facilitate the planning, implementation, monitoring and on-going development of corporate IT security.

**Professional IT security solutions require professional IT security experts.**



## CTO Comment Box

The lives of CIOs are not becoming easier. Cost pressure increases, the IT's contribution to business is expected to grow, while agility and complexity of the daily business processes are rising as well. The IT is expected to be a driver, but is often driven itself, partly by the company departments, but also partly by the trends of the markets.

The old maxim "enterprise drives consumer" is no longer valid, the opposite is the case. The iPhone began its triumphal march outside the companies, but which CIO wanted to have it anyway?

But when the CEO happily entered the office, holding an iPhone in one hand and an Android smartphone in his other hand, this most of the time meant the end of the proven single-device strategy.

The challenge the IT must face is to manage this ever-increasing complexity without forgetting about basic requirements such as availability and security. The solutions to this problem is probably to manage and to integrate all these developments in an active and intelligent way; proactively and not reactively, a deep know-how of one's own business, the right partners and a smart usage of innovations and developments like multifactor security concepts, new security technologies etc. The awareness in companies of security threats however is often far behind reality.

Still, IT security is considered a part of compliance, and the increasing threatening situation of the cyber war of the international competition is ignored.

Several countries openly admit that they are engaged in industrial espionage and consider it a legitimate part of their own economic master plans. A change of mind in the highest levels of the companies to prevent the loss of vital advantages in competition is of utmost importance.

### 3 NewsWatch

The GFT NewsWatch will henceforth follow the professional article on a monthly basis, covering major events, vendor announcements, service and products launches, important mergers and acquisitions, etc. related to the IT industry. Thereby, the NewsWatch is based on international releases of the past month.

#### RSA® Conference Europe 2010 announces keynote speaker line-up for its Annual Conference in October

Source: <http://www.businesswire.com/news/home/20100713005872/en/RSA%C2%AE-Conference-Europe-2010-Announces-Keynote-Speaker>

RSA Conference, the world's leading information security conference group, announced its line-up of keynote speakers for RSA® Conference Europe 2010, taking place from 12th -14th October 2010, at the Hilton London Metropole Hotel, UK.

#### BlackBerry access deal 'ready' in India

Source: <http://www.guardian.co.uk/technology/2010/aug/17/blackberry-access-india>

BlackBerry manufacturer Research In Motion will allow Indian authorities partial access to its Messenger chat services to placate security fears.

#### Drugstore Schlecker customer information exposed on web

Source: <http://www.thelocal.de/national/20100827-29437.html>

German drugstore chain Schlecker has suffered a major online data breach, with the names, addresses and profiles of about 150,000 customers being exposed on the internet.

#### CA Technologies buys Arcot Systems

Source: <http://www.computerweekly.com/Articles/2010/09/06/242621/CA-Technologies-buys-Arcot-Systems-for-163129m.htm>

CA Technologies will extend its cloud security services with the acquisition of fraud prevention company Arcot Systems. The \$200m (£129m) acquisition will add Arcot Systems' software-only credit card fraud prevention and authentication technology to CA Technologies's identity and access management (IAM) offerings.

#### Gartner reveals key Customer Relationship Management predictions for 2010

Source: <http://www.gartner.com/it/page.jsp?id=1305714>

Facebook will be the No. 1 social network in all but 25 countries, according to Gartner, Inc. In countries such as Brazil, Russia, India, China and Japan it will not be No. 1. The prediction is one in a series Gartner analysts have made on customer relationship management (CRM) in areas including CRM marketing and social CRM.

### Deutsche Post consolidates involvement in online advertising market and acquires nugg.ad AG

Source: [http://www.dp-dhl.de/en/media\\_relations/press\\_releases/2010/deutsche\\_post\\_acquires\\_nugg\\_ad.html](http://www.dp-dhl.de/en/media_relations/press_releases/2010/deutsche_post_acquires_nugg_ad.html)

In taking over nugg.ad AG, Deutsche Post AG is acquiring Europe's largest targeting platform and in so doing has expanded its competence as a service provider in the on-line advertising market.

### Google buys Like.com

Source: <http://tech.fortune.cnn.com/2010/08/20/google-buys-like-com/>

Like.com announced on its site that it had agreed to be picked up by Google. The shopping site allows users to search for jewelry, handbags, shoes, and watches. It makes money on affiliate links which are estimated to be as high as 10%.

### Intel buys cyber security giant McAfee for \$7.68 billion in cash

Source: <http://techcrunch.com/2010/08/19/intel-buys-cyber-security-giant-mcafee-for-7-68-billion-in-cash/>

Intel has just bought computer and software security company McAfee. The all cash deal is worth \$7.68 billion, or \$48 per share.

### BlackBerry App World 2.0 leaves beta, includes cheaper apps and new payment options

Source: <http://www.engadget.com/2010/08/20/blackberry-app-world-2-0-leaves-beta-includes-cheaper-apps-and/>

The latest version of BlackBerry App World is now available, including a number of welcome additions, for example, RIM has dropped the \$2.99 minimum from paid apps, so now BlackBerry developers can release \$0.99 and \$1.99 apps just like everybody else.

### Intel and Nokia create first joint laboratory

Source: [http://newsroom.intel.com/community/intel\\_newsroom/blog/2010/08/23/intel-and-nokia-create-first-joint-laboratory](http://newsroom.intel.com/community/intel_newsroom/blog/2010/08/23/intel-and-nokia-create-first-joint-laboratory)

Intel Corporation, Nokia and the University of Oulu officially opened the Intel and Nokia Joint Innovation Center today. It will employ about two dozen R&D professionals and become the latest member of Intel's European Research Network, Intel Labs Europe.

### Gartner BPM Hype Cycle 2010

Source: [http://www.gartner.com/DisplayDocument?doc\\_cd=205839&ref=g\\_rss](http://www.gartner.com/DisplayDocument?doc_cd=205839&ref=g_rss)

The 2010 Gartner Hype Cycle Special Report evaluates the maturity of 1,800 technologies and trends in 75 areas. New this year are business use of social technology, sustainability and green IT, emerging energy technologies, enterprise architecture, Pattern-Based Strategy, and performance management.

### HP pays \$55 million to settle kickback scandal

Source: <http://www.zdnet.com/news/hp-pays-55-million-to-settle-kickback-scandal/461573>

Hewlett-Packard has agreed to pay the U.S. government \$55 million to settle charges that it paid kickbacks to technology partners for recommending HP products to federal agencies.

### HTC files answer in Apple patent lawsuit

Source: [http://www.macobserver.com/tmo/article/htc\\_files\\_answer\\_in\\_apple\\_patent\\_lawsuit/](http://www.macobserver.com/tmo/article/htc_files_answer_in_apple_patent_lawsuit/)

HTC files its answer to Apple's patent infringement lawsuit in Delaware with the expected denial that it has done anything wrong and also claimed that four of Apple's patents are invalid. Apple filed two lawsuits against HTC alleging some of the smartphone maker's products infringe on no less than 20 of its iPhone-related patents.

### Microsoft's Bing search tops Yahoo

Source: <http://content.usatoday.com/communities/technologylive/post/2010/09/microsofts-bing-search-tops-yahoo/1>

For the first time, Microsoft's Bing search engine has more U.S. users than Yahoo, researcher Nielsen said today. In August, Bing had 13.9% of the U.S. search market, compared to 13.1% for Yahoo.

### XpanD's Universal 3D shutter glasses to work on most displays

Source: [http://www.pcworld.com/article/191682/xpands\\_universal\\_3d\\_shutter\\_glasses\\_to\\_work\\_on\\_most\\_displays.html](http://www.pcworld.com/article/191682/xpands_universal_3d_shutter_glasses_to_work_on_most_displays.html)

XpanD's X103 glasses will be compatible with most computer monitors and 3D TVs, as well as all cinemas currently using XpanD's technology. XpanD is using the standard active shutter-glasses technology that most 3DTV manufacturers employ with their new 3D models.

### Apple presents a music social network Ping

Source: <http://www.playgroundmag.net/noticia/13667/apple-presents-ping-an-itunes-social-network-for-music>

Steve Jobs, CEO of Apple has announced the creation of a music social network, Ping. MySpace was the first social network in the United States in 2006 and the rendezvous for the music lovers on the web. Ping has been designed to change the user experience on iTunes.

### To 100 million and beyond with Google Maps for mobile

Source: <http://googlemobile.blogspot.com/2010/08/to-100-million-and-beyond-with-google.html>

Today, more than 100 million people a month are now using Google Maps for mobile to get from point A to point B, find nearby places, and more.

### Apple planning \$0.99 iTunes TV rentals?

Source: <http://www.digitaltrends.com/mobile/apple-planning-0-99-itunes-tv-rentals/>

Unconfirmed reports have Apple in talks with News Corp and others about offering 48-hour rentals of popular television shows for \$0.99.

### Google testing voice calling in Gmail

Source: [http://news.cnet.com/8301-30684\\_3-20014617-265.html](http://news.cnet.com/8301-30684_3-20014617-265.html)

Google could be ready to turn Gmail into a communications hub by adding the ability to make phone calls from the Google Chat interface.

### Spending on Software Testing rise to € 100 billion by 2014

Source: [https://www.pac-online.com/pac/pac/live/pac\\_world/sitsi\\_market\\_research/search\\_reports/info\\_rapport/index.html?lenya.usecase=show-info-rapport&document=/pac\\_sitsi\\_reports/local\\_report/WW\\_Testing\\_GlobalView\\_10/index.xml](https://www.pac-online.com/pac/pac/live/pac_world/sitsi_market_research/search_reports/info_rapport/index.html?lenya.usecase=show-info-rapport&document=/pac_sitsi_reports/local_report/WW_Testing_GlobalView_10/index.xml)

Global spending on Software Testing is to rise to € 100 billion by 2014 according to analysts from Pierre Audoin Consultants (PAC) in their study "Worldwide Testing Services Market 2010-2014: Key Growth opportunities & Sector Trends". Thus, the software testing area is the area with the highest growth rate for the entire IT market.

### New Kindles set Amazon sales records

Source: <http://www.fiercecontentmanagement.com/story/New-Kindles-set-Amazon-sales-records/2010-08-31>

Amazon released the first four-week sales figures for its new generation of Kindle eBook readers saying that there were record orders for the latest group of Kindles.

