Securing
our **connected** world

www.tmforum.org
2013

tmforum SECURITY AND DEFENSE PUBLICATION

SECURING THE CYBER SUPPLY CHAIN

Why standards and maturity matter

APPLYING THE 80:20 RULE TO CYBER OPERATIONS

PATCH MANAGEMENT AND PUBLIC SERVICES

DEVELOPING METRICS FOR ASSESSING SECURITY

Securing our connected world

TM Forum's research reports are free for all employees of our member companies to download by registering on our website.

Publications Managing Editor:
Annie Turner
aturner@tmforum.org

Contributors:
Dr. Sandor Boyson, Robert H. Smith School Of Business, University of Maryland
sboyson@rhsmith.umd.edu

John Williamson, Editor, *Jane's Military Communications*
john.williamson20@btopenworld.com

Editor:
Claire Manuel
cmanuel@tmforum.org

Creative Director:
David Andrews
dandrews@tmforum.org

Business Development Director, Research & Publications:
Mark Bradbury
mbradbury@tmforum.org

Business Development Director, Research & Publications:
Nick Carter
ncarter@tmforum.org

Senior Publisher:
Katy Gambino
kgambino@tmforum.org

Production Assistant:
Aideen Greenlee
agreenlee@tmforum.org

Head of Marketing:
Lacey Caldwell Senko
lsenko@tmforum.org

Report Design:
The Page Design Consultancy Ltd

Vice President, Research & Publications:
Rebecca Henderson
rhenderson@tmforum.org

Advisors:
Keith Willetts, Non-executive Chairman, TM Forum
Martin Creaner, President and Chief Executive Officer, TM Forum
Nik Willetts, Chief Strategy Officer, TM Forum

Published by:
TM Forum
240 Headquarters Plaza
East Tower, 10th Floor
Morristown, NJ 07960-6628
USA
www.tmforum.org
Phone: +1 973-944-5100
Fax: +1 973-944-5110

Contents

THE YEAR IN FOCUS:
SECURING THE SUPPLY CHAIN, PROTECTING ORGANIZATIONS' FIVE GREATEST VULNERABILITIES

THE TERM OF ADVANCED persistent threat was coined by the U.S. Department of Defense in 2006 to describe state-sponsored cyber attacks. It has come to describe the fact that almost every organization's IT systems face a constant onslaught for a variety of reasons and from many sources.

In response to this growing, persistent threat, since last year's edition of *Securing our connected world*, TM Forum has formally recognized cyber security as being an essential core competency for all types of service providers and has focused its security efforts in two areas. First looking at how to strengthen the supply chain – any structure is only as strong as its weakest link. Until relatively recently, just how many systems, processes and parties make up that chain and how the combination of them can be exploited was not well understood.

We are fortunate to have a leading expert in this increasingly important field, Dr. Sandor Boyson, Director and Research Professor for the Supply Chain Management Center, Robert H. Smith School of Business at the University of Maryland, outline issues and thinking on the cyber supply chain in this edition, on page 6.

Second the Forum's security management team has worked hard, developing best practices to make the greatest impact in the most economic (in every sense) and pragmatic way. They are addressing issues in five key areas, which they identified by researching and assessing other, specialist organizations' work, across which they discovered much commonality. They are:

- patch management;
- human factors;
- mobile device management
- distributed denial of service (DDoS) mitigation; and
- server hardening.

Part of that commonality was that the Pareto Principle, also known as the 80:20 rule applies: That is, in this context, 80 percent of all cyber security problems could be prevented taking 20 percent of the precautions available. You'll find a brief article about each of these crucial areas and how the Forum's dedicated team has been and is addressing them, as contributions to and in support of our Frameworx suite of standards-based tools and best practices.

A main thrust of this initial work was developing key performance indicators to help organizations measure how effective their security precautions are – to gauge operational assurance – which is in great contrast to the usual approach of assessing and measuring things when they go wrong.

TM Forum acknowledges our debt to the defense industry in getting our security efforts started in earnest and helping us with the ongoing process of embedding security in Frameworx (see page 21 for details). It is most gratifying to find that in turn the defense industry recognizes the value of Frameworx.

This was demonstrated during 2012 when the U.S. Department of Defense (which is a member of the Forum) issued a new network management policy for its communications suppliers and system integrators that requires TM Forum's Information Framework (SID), a key element of Frameworx, as one of its baseline protocols and standards for exchanging network management data.

This is known as the Network Management (NM) Instruction DODI 8410.03[1]. The policy also references TM Forum's *Service Level Agreement Management Handbook*, Release 3.0 (GB917)[2]. It provides a full set of definitions used in the field of managing SLAs, which are widely used in many industry sectors today.

On that note, in September and October 2012, TM Forum conducted its second annual survey to measure adoption of Frameworx. The survey had 87 respondents, 70 percent of whom are in the world's top 100 communication service providers. It found 91 percent of participants are using Frameworx and 72 percent of them mandate Frameworx in many or all of their specifications, up from 63 percent in 2011.

In addition, 75 percent of all the respondents who mandate Frameworx during procurement said that whether or not a product or solution conforms to standards, it is an important influence on their purchasing decision. This puts the companies who have earned the valued TM Forum Frameworx Conformance Certification Mark for their solutions or products in a strong position.

Further, 83 percent of all respondents agreed that Frameworx plays a key role in enabling the deployment of new services and 66 percent said it will play an important part in delivering digital services.

TM Forum grants a TM Forum Conformance Mark to all products and solutions that successfully complete the Frameworx Conformance Certification assessment process and publish their results. TM Forum also announces the completed certification to its membership base of over 65,000 individuals from 900-plus companies around the world. Suppliers are then free to use the Conformance Mark in their own marketing efforts.

We hope you enjoy this edition of *Securing our connected world* and find it both useful and interesting.

Martin Creaner
President & CEO
TM Forum

[1]For more information, please go to www.dtic.mil/whs/directives/corres/pdf/841003p.pdf.
[2]The Handbook is free to TM Forum's members to download from our website from www.tmforum.org/GB917SLAManagement

THE CYBER-SUPPLY CHAIN: SECURITY'S NEW FRONTIER

Dr. Sandor Boyson
Director, Supply Chain Management Center and Research Professor
Robert H. Smith School Of Business, University of Maryland

IN 2007, HARD DRIVES produced in Thailand had a Trojan horse pre-installed, which acted as report-back mechanisms to a foreign intelligence service. They found their way into U.S Department of Defense IT systems.

In 2010, Dell PowerEdge 410 servers were shipped with malware pre-installed on their motherboards, requiring 16 changes in supply chain procedures to cut off the attack path. These examples highlight why securing the cyber supply chain has become a strategic priority for policy makers and practitioners.

In the U.S., the President's Comprehensive National Cybersecurity (CNCI) Initiative and the White House's National Strategy For Supply Chain Security (released in January 2012) have both addressed this urgent issue.

In support of the CNCI, the University of Maryland's Robert H. Smith School Of Business' Supply Chain Management Center and its sponsor, the National Institute of Standards and Technology (NIST), have conducted rigorous ICT supply chain risk management research and industry outreach over the past three years.

In the first stage of our research, we conducted the first of its kind survey of over 200 ICT companies, of all sizes, which are vendors to the federal enterprise.

It was sponsored by NIST and called *Assessing supply chain risk management capabilities and perspectives of the IT vendor community: toward a cyber-supply chain code of practice*[1].

Based on the results, we built a model of the ICT supply chain and profiled vendors' capabilities regarding supply chain risk management.

In the second stage, we created an ICT supply chain risk management Reference Architecture. This is an integrative model which sought to address the dual challenges of assuring defense in breadth and defense in depth.

Defense in breadth is extensive: It covers the whole business ecosystem of system acquirers, integrators, suppliers and their key, shared processes. Defense in depth is intensive: it covers risk governance; systems lifecycle management (including design, risk assessment and supply base modeling/ auditing); and operations management.

In the third stage of our research, we employed this Reference Architecture to evaluate over 60 industry and public sector supply chain risk management initiatives in software, hardware, network and system integration services. The Architecture enabled us to position these initiatives against a comprehensive, end-to-end model; and to facilitate the identification and assessment of gaps in coverage in the ICT supply chain risk management discipline. Sample initiatives are shown in Figure 1.

Figure 1 shows a clear clustering of efforts around the internally-oriented systems

"Defense in breadth is extensive: It covers the whole business ecosystem. … Defense in depth is intensive: it covers risk governance, systems lifecycle management and operations management."

development and supplier-oriented sourcing functions.

At the high end of the defense in depth axis, there appear to be big gaps in various initiatives' coverage of risk governance. In fact, deficiencies in the enterprise risk management function prevent the coordination of adequate defense in breadth measures across the extended supply chain.

This deficiency is not just at the initiative-level; it also at the operational firm-level.

From our NIST-sponsored Survey, we found that:

- On the strategic side of risk management, 47.6 percent of our sample of 200 companies never use a risk board or other executive mechanisms to govern risk;
- 46.1 percent never use a shared risk registry, that is, an online database of IT supply chain risks;
- 49.4 percent never use an integrated IT supply chain risk management dashboard; and
- 44.9 percent say they never use a supply chain risk management plan.

At the other end of the defense in depth axis, there are coverage gaps at the lowest level of field operations. Many ICT initiatives (and companies themselves) do not address the need for automated business rules and sensor-driven responses so, for example, they cannot sense and respond to risks in real time.

Our research has led to one inescapable conclusion: the cyber supply chain today is as fragmented and stovepiped today as the physical product supply chain was in the mid-1990s.

In an earlier work, *Toward a cyber-supply chain code of practice* (published by NIST, March 2011), we concluded: "The cyber supply chain discipline is currently in an emerging state characterized by: a deficient evidence-based body of knowledge; a proliferation and fragmentation of industry best practices and standards groups, generally led by only the largest firms; and a profound under-usage of supply chain-wide risk governance mechanisms inside IT vendors." (p.45)

There is an urgent need – expressed by the majority of participants in our focus group over the past three years – for a formal ICT supply chain risk management community, a public/private partnership to speed up the development of a knowledge base and a set of effective practices. Such a partnership could perform a more detailed mapping of supply chain risk management initiatives to identify inconsistencies in approaches that the partnership can help reconcile; and complete a guidance document for using multiple frameworks/standards to achieve a comprehensive ICT supply chain risk management program.

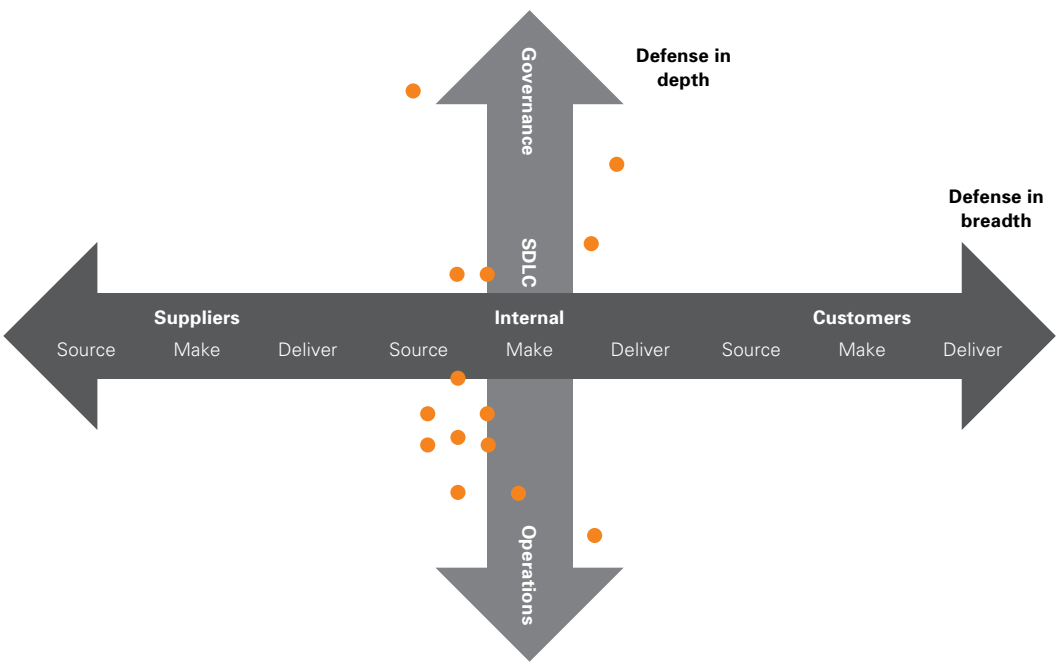
This community also needs a capability/maturity model that it can trust to guide its actions along an increasingly complex, evolutionary growth path and underpin its supply chain assurance investments with a solid foundational logic.

Towards that end, the Supply Chain Management Center of The Robert H. Smith School Of Business, University Of Maryland, has just completed its latest phase of research for NIST. It has also developed an Enterprise ICT Supply Chain Risk Management (SCRM) Capability/Maturity Assessment Package as a proof of concept.

This Package is delivered through a secure ICT SCRM Portal, with four major functions:

- an initiatives section with summaries of major public and private sector ICT SCRM initiatives, which can be updated;

Figure 1: Clusters around defense in breadth and defense in depth



Have you seen our other recent TM Forum publications?

TM Forum's research reports are free for all employees of our member companies to download by registering on our website. The reports are also available for non-members to purchase online.

Real-time convergent charging: Adapting to the digital environment

For the first time in a long time, service providers are faced with a technology choice that doesn't depend on reducing the cost of operations as its primary benefit. Calling real-time convergent charging (RTCC) a revenue management solution is like calling James Bond a civil servant: The underpinning technology has extended to include converged services, customer interactions and service delivery.

This TM Forum *Insights Research* report shows why and how RTCC should be a priority for service providers. Through a series of in-depth interviews with operators from across the globe, we discover just how far they have come in transforming their businesses into agile and creative competitors using the tools supplied by RTCC and the ecosystems sprouting up around it.

The report concludes that operating in the way RTCC enables is like eliminating the word "no" from the CIO's vocabulary.

Connected home: Does cable hold the key?

Cable companies are facing fierce competition from cheaper, IP-based offerings, and are looking to the concept of the connected home to generate new revenue streams and broaden their appeal to customers. This report looks at how they are placed to exploit their position in the home to become the connected home service provider of choice.

Their big advantages are their brand and the fact that they've been able to extend their portfolio (offering broadband and, in places, free Wi-Fi hotspot access for instance) more easily than 'native' communications service providers have found it to move into providing entertainment.

Many challenges remain, including identifying the best-fit partners for a whole range of potential services – from personalized TV channels, to eHealth, security and remote control of everything from the oven to air con and future services such as pet monitoring, advanced social networking, music services – and running those partnerships successfully, including developing viable, sustainable business models that work for all parties.

Middle East Insights: From rapid growth to maturity – strategies for sustainability

Produced in collaboration with Informa Telecoms & Media, this Regional Insights report explores why the Middle East region offers better growth prospects than many others, despite maturing markets and the continuing tough economic conditions.

The most fervent competition is in mobile and although the rate of growth is slowing, having almost halved between its peak at 24.4 percent in 2009 to 13.1 percent in 2012, operators in technologically advanced countries like Saudi Arabia still enjoy strong revenue growth.

Operators looking to differentiate themselves are particularly turning to their high-value customers. We investigate how they are approaching issues like segmentation; introducing new services; sourcing fresh, local content; working with over-the-top players; better serving the enterprise market; and using VoIP and machine-to-machine communications.

The report explores the range of bespoke plans (with many examples) from operators, developed to attract and keep customers and looks at investment in infrastructure, including LTE, across the region. Although it will be sometime before LTE will be a mainstream technology, the rapid take-up of mobile broadband as soon as it is available is a clear indicator of pent-up demand.

Visit **www.tmforum.org/researchpublications** to find out more

- a library with a spectrum of related policy studies, case studies, research reports, and so on;
- a Forum which enables collaboration groups to form around specific ICT SCRM topic areas; and
- an enterprise assessment section.

The enterprise assessment section has:

- a strategic readiness tool which profiles an enterprise's risk management posture and organizational development status;
- a NIST principles/practices tool that drills down into the 10 major ICT SCRM principles embedded in NIST IR 7622 and asks a portfolio of operational questions associated with each principle;
- a cyber chain mapping tool, which provides a rapid method to build a working global map of cyber supply chain assets, transactions and vulnerabilities; and
- a results area that enables enterprises to view their ICT SCRM baseline status against three benchmarks. They are a group of peer enterprises; the Community Framework Model; and an ICT SCRM Capability/ Maturity Level.

TM Forum supported our assessment development activities for field testing the assessment tools. It selectively recruited a small pool from its members to validate our survey instruments and provide feedback.

Three large, commercial service providers from North America, Australia and Europe took the survey and provided feedback. There were considerable differences between respondents in many areas of ICT SCRM, as demonstrated in Figure 2, regarding who contributes to risk management policy in each organization.

After completing the survey, the respondents' answers were scored for their capabilities and maturity in cyber-supply chain risk management as follows:

- Emergent Phase, meaning limited planning and implementation of critical cyber supply chain risk management factors, with stove piped efforts.
- Diligent Phase describes steady efforts to enact supply chain controls, with emphasis on enterprise integration.
- Proficient Phase details the seasoned implementation and improving processes across the extended supply chain, including enterprise partners.

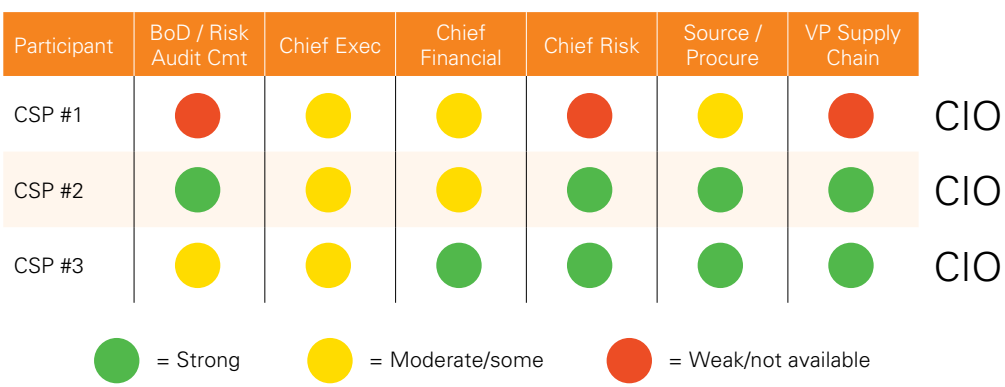
The respondents found this to be most useful, because the tool also provided recommendations for improvement based on the capability and maturity level.

Overall, the respondents seemed pleased with the experience. As one noted, "We… found it very useful with lots of food for thought".

Christy Coffey, Director, Industry & Security Programs, TM Forum, came to our October 16 2012 NIST Workshop to demonstrate the portal. She presented this feedback to the workshop audience, which was composed of leaders from many areas of cyber security.

This kind of collaboration between university, industry and government will be increasingly vital as we collectively seek to secure the global cyber-supply chain against escalating risks and threats.

Figure 2: Who contributes significantly to developing policy for cyber risk management?



Source: Cyber risk management readiness survey, TM Forum 2011

CYBER SECURITY: DOING THE RIGHT THINGS

As almost every nation's dependencies on access to advanced IT and networking systems grow, so do the negative consequences of unauthorized access to and disruption of those systems. The same applies to commercial and other organizations: The cost of systems being compromised is already huge – and rising.

AT ONE END OF THE spectrum, according to the *2012 Cost of Cyber Crime Study*, an analysis conducted by the Ponemon Institute, sponsored by HP, the average annualized cost of cyber crime incurred by a benchmark sample of U.S. organizations was $8.9 million.

This represents a 6 percent increase over the average cost reported in 2011, and a 38 percent increase over 2010. At the other end of the scale, as shown by the experiences of organizations and institutions in Australia, Estonia, Israel, Iran, Saudi Arabia and others, cyber warfare attacks have the potential to seriously challenge a nation state's ability to function normally.

Little things mean a lot

The good news is that some effective security technologies and mechanisms have been developed over time to warn of, protect against and recover from cyber attacks.

In practice, many experts and analysts have concluded that paying closer attention to the security basics can mitigate the majority of the root causes of cyber threats and risks: it's suggested that something like 20 percent of countermeasures implemented effectively can prevent 80 percent or more of the attacks.

This sort of message is contained in studies such as the Australian Defence Signals Directorate's *Top 35 Mitigation Strategies, and the Data Breach Investigations Report* lead-authored by U.S. operator Verizon.

"The evidence from computer emergency response teams around the world is that a few basic controls will mitigate most of the threat as it currently exists," states Martin Huddleston, a Cyber Defence Capability Advisor to the U.K. Ministry of Defence.

So what are the cyber basics that it pays dividends to get right? Huddleston, who is also a technical champion in Cyber Security, Management Systems and Cyber Solutions Architecture at the U.K. Defence Science and Technology Laboratories (DSTL)[1], notes the guidance provided by the UK Government's *10 Steps to Cyber Security* analysis. In summary, this recommends paying greater attention to areas such as:

- home and mobile networking policies;
- user education and awareness;
- incident management
- information risk management
- user privilege management;
- control of removable media;
- ICT systems and network monitoring;
- secure configuration of systems;
- malware protection;
- internal and external network security.

Patch work

As part of the 'Secure configuration of systems' above, patch management – the administration and supervision of the processes and technology for keeping systems updated with the latest security software defenses – is commonly included in lists of basic security must-haves. "It also provides essential

"Many experts and analysts have concluded that paying closer attention to the security basics can mitigate the majority of the root causes of cyber threats and risks."

protection against malware," observes Huddleston.

But just because it's a basic requirement doesn't necessarily make patch management simple to implement. The process can be costly, time- and labor-intensive, and quite complex for large organizations running an extended inventory of disparate hardware and software systems that is commonly spatially distributed. That is distributed heterogeneous systems at the enterprise level. One challenge is to conduct patch management without causing disruption to business or other operations.

"To make patching effective you need a combined policy that covers security, maintenance and other provisioning activities that are going on in the network," adds Huddleston. "The crux of the patching issue is how to maintain a secure profile while allowing your organization to do those other things such as maintenance and provisioning."

Then there's the matter of measuring how effective patch management actually is. Here, a new TM Forum publication, *Quick Start Pack: Patch Management (GB965)*[2], is designed to eliminate guesswork.

This document is one of several that have resulted from TM Forum's Cyber Operations teams studying the various metrics that might be applied to contracting for, and provisioning of, some of the components that are essential for improved cyber security, as the subsequent articles in this publication outline.

"We've critiqued a vast range of metrics from all sorts of sources and settled on six that provide real value to the security story," explains Huddleston, who was heavily involved with TM Forum's patching metric initiative. The Forum's six patching metrics are as follows:

- the length of time that the system/device has been unpatched and exposed;
- the percentage of devices by percentage that are actually patched;
- the criticality of patch exposure;
- the audited degree of system susceptibility to attack;
- the percentage of patches that result in further security problems, or the mean time between failure of patch security;
- the number of patches that are in use.

Huddleston argues that to achieve their optimum value, these metrics should be used in combination. For example, the second in the list above might give an organization a feeling for how well it's covered, but the percentage that's left doesn't really tell the organization what degree of risk it's carrying.

However, if the second metric is paired with the fourth metric, and the percentage that isn't patched isn't susceptible to attack, then the organization probably has a very good security posture.

In addition to metrics and benchmarking for other security basics such as distributed denial of service (DDoS) countermeasures, human factor mitigation and mobile device management, TM Forum activity that's applicable to overall cyber security ranges from work on revenue assurance – with its connection to fraud management – to securing the enterprise cloud.

Future phases of TM Forum's CyberOps Metrics projects are expected to include collaboration on metrics to support whitelisting (where only approved code can run), user privileges and bring your own device (BYOD) mobile working. The Forum has a Catalyst project to demonstrate and jump-start technical solutions for cyber security challenges focused on Threat Intelligence Sharing.

This project has identified two initial use cases, Mobile Malware and APT Targeted Attack, and hopes to show that real-time sharing of Threat Intelligence between trusted partners can be the new reality given a combination of standards and COTS products.

Going public

Meantime, a telling accolade to TM Forum's work on patch management has been paid with the inclusion of referencing of the GB965 mitigation guidelines in the UK Government's Public Sector Network (PSN) initiative, a project that is aimed at unifying the various different legacy public sector ICT networks into one, standardized logical network.

The ambitious PSN undertaking is planned to connect up to 4 million public sector workers using PCs – some 80 percent of the total – by 2014, in the process saving up to £130 million annually in procurement and networking costs.

The use of GB965, referenced in the PSN's own common standard for Malware Protection alongside the *10 Steps to Cyber Security* will provide guidelines that can be used by PSN service providers and users to better agree contracts, monitor network activity and publish information on security postures.

And for the future, Huddleston envisages that patch management along with other controls in the '10 steps to cyber Security' could become something of a low-cost, default inclusion in IT systems and operations.

"I see patch management developing so that it can be automated, and vendors can embed it and make it simple and easy for user organizations," he concludes.

"We need to try and operationalize these basic controls to the degree that they are a de facto standard in all the software that's used, out of the box, and they become commodities and not a major overhead."

[1]www.gchq.gov.uk/Press/Pages/10-Steps-to-Cyber-Security.aspx
[2]*Quick Start Pack: Patch Management* (GB965) can be downloaded free by all employees of TM Forum's member organizations who register on the website from www.tmforum.org/GB965CyperOPsMetrics

PICK YOUR OWN BATTLEGROUND?

Wireless mobility is transforming the procedures and scope of many aspects of modern life, impacting anything and everything from commerce and banking to healthcare and entertainment. Nowhere are the positive effects of the technology more evident than in the enterprise, with the mobilization of the workforce having the potential to simultaneously cut costs, increase efficiencies and achieve a better balance between work and leisure time. However, it also has the potential to compromise an organization's IT infrastructure, operations and data.

UNFORTUNATELY, INCREASED security vulnerabilities are part and parcel of the wireless mobility deal, with mobile devices offering an incomplete, dynamic and complex environment that is an attractive habitat for hackers.

Again, this is arguably most evident in the enterprise where mobile systems can be compromised, malware inadvertently imported on mobiles, and devices containing high-value and/or sensitive data lost or stolen.

Now a new security battlefront is opening up with the rise of the phenomenon known as bring your own device (BYOD), or bring your own technology (BYOT), in which employees use their own mobile devices rather than those provided by the enterprise.

Although some of the apparent advantages of BYOD are disputed, evangelists for the practice list improved productivity, lower costs, greater employee satisfaction and potentially speedier technology refresh among its attractions.

Certainly great things are forecast for BYOD. According to a recent MarketsandMarkets analysis[1], the total BYOD and enterprise mobility market is expected to reach $181.39 billion by 2017.

Risky business

You can readily see, though, how security concerns can start to multiply and intensify with the BYOD proposition. The proliferation of device types in operation, the differing degrees of vulnerability of different operating systems, and the mixing of personal with corporate data, can add up to a major security management headache.

"If managing a corporate device without compromising its usability was a hard task when all employees had similar devices (such as BlackBerrys), it has become an even harder task now that employees have their personal data mixed in with work information in smartphones they acquire themselves," pointed out Senior Analyst Vinicius Caetano in a Pyramid Research note posted in November 2012 on RIM's repositioning of its Mobile Device Management (MDM) offering.

"By not creating the appropriate policy and framework for people to use personal devices, companies are creating a bigger risk, as people will find their own ways of transferring corporate data to devices, methods which are often very risky," adds Alan Carter, Solutions Consultant at IT

"By not creating the appropriate policy and framework for people to use personal devices, companies are creating a bigger risk, as people will find their own ways of transferring corporate data."

security service provider SecureData. "This may be done to allow people to work from their own devices, and while not malicious, it could leave the company open to security breaches, which could include the loss of highly sensitive data."

Meantime, if 'jail broken' devices, with software modified from its original form to allow new apps to be run or operation on new networks, are factored into the equation, security management problems can be compounded.

On the upside, though, there are a number of weapons to hand to minimize the potential security weaknesses of BYOD.

"Enterprises have a number of options available to ensure that mobile devices do not pose a risk to their data security, including device and application authentication, remote locking and data deletion from lost devices and partitioning of devices for business and personal use," observes Patrick Rusby, Research Analyst, Analysys Mason.

Not left to their own devices

Such measures, along with policy management, logging and the application of relevant metrics, are elements of mobile device management (MDM). This is a business opportunity variously estimated to be worth between $1.1 billion by year-end 2016 (The Radicati Group) and $6.6 billion by 2015 (Forrester Research). MDM is also an opportunity open to mobile network operators and communication service providers, as well as security and IT firms.

"Mobile device management is being increasingly demanded by enterprises. We recommend that mobile operators look to provide MDM services to their enterprise and SME customers, as part of an overall strategy to manage reducing revenues from core voice services, and to reduce enterprise customer churn," says Rusby.

He adds, "Communication service providers should look to offer cloud MDM services to their enterprise customers, as it is a natural fit with providing mobile voice and data services. Enterprises may not instinctively choose their mobile operator as their provider of IT services, however, so operators should look to partner with best-in-class MDM vendors to reassure their customers."

As might be anticipated, the implementation of effective MDM strategies and systems is itself not without its own set of problems and challenges.

One issue is the attitude of some users. "Many employees want to use their own devices at work, and employers are right to think about what this means for their data security. While an employee can hardly complain about MDM on their corporate-liable device, their personal device may be another matter," ventures Rusby. "Any MDM solution for personal devices would have to be very subtle to be accepted."

Another is potentially high cost. Solutions that aim to address all potential security management eventualities, manage all device operating systems, and accommodate the large numbers of different devices that can be involved are expensive and highly complex. If you add in a complete set of BYOD requirements, it becomes even more so.

Consequently MDM is being revisited in the wake of the unstoppable popularity of BYOD and this new thinking is likely to be unfamiliar to many enterprises.

TM Forum identified MDM was one of the five most important security vulnerabilities faced by enterprises (see page 4).

It has recently published the TM Forum *Quick Start Guide: Mobile Device Management*[2], which provides expert insights into best practices for MDM plus an extended array of metrics that can be used to chart the effectiveness of an enterprise's MDM capabilities.

A pragmatic guide

The publication is a pragmatic guide to security in an enterprise's network. It could also enable an enterprise to determine what its user base is doing with mobile devices, at least insofar as it affects the organization's valuable data and access security.

The Guide references:

- the Australian Defence Signals Directorate's top 35 strategies to mitigate targeted cyber intrusions;
- the 20 critical security controls for effective cyber defense and audit guidelines developed by the U.S. SANS Institute; and
- the general practices of the U.S. National Institute of Standards and Technology and the International Organization for Standardization.

It also acknowledges studies by Gartner, Forrester and other research groups, and the direct contributions of TM Forum participants and members, including the U.S. Defense Information Systems Agency, NATO, the U.K.'s Ministry of Defence, and their contractors.

The Guide is published at an opportune moment. As Carter concludes: "Smartphones and tablet devices are not going away, and neither is the risk to corporate data held on these devices."

[1]Bring-your-own-device Market (BYOD), Consumerization of IT (Co-IT) and Enterprise Mobility Market – Global Advancements, Business Models, Market Forecasts & Analysis (2012 – 2017), see www.marketsandmarkets.com/Market-Reports/enterprise-mobility-334.html for more information

[2]The Guidebook is available from here to all employees of our members organizations who register on our website from here www.tmforum.org/GB966CyberOpsMetrics

HOW TO AVOID BEING IN DENIAL

Distributed denial of service (DDoS) is a phenomenon rarely out of the news. There is a steady rise in the reported incidence of DDoS attacks on the websites of banks, other businesses and governmental agencies. Websites are overwhelmed by too many requests at once, often causing them to crash. Leaving aside the interruption to service, there are a number of serious, harmful consequences that can result from successful malicious DDoS attacks. Some basic measures can make a huge difference.

SERVICE IS NOT ALWAYS denied as the result of any malicious intent, but as a consequence of poor system design, meaning that sites cannot cope with out-of-profile volumes of traffic triggered by certain events. In many cases, though, request storms are spurious, motivated by malicious intent to degrade service levels or prevent the site servicing legitimate requests.

There's the obvious potential for financial loss arising from the inability to transact normal business, and there are clear national security implications attached to utility and governmental websites being forced offline.

However, according to Mike Carpenter, Vice President, Service Assurance at enterprise mobility software specialist TOA Technologies, the threats posed by DDoS attacks themselves might be less critical than their consequences.

These include the other attacks which DDoS episodes can help to disguise when defenses are overloaded, loss of reputation when legitimate requests are blocked, and undermining key assumptions about 'Internet availability', as shown by the increased number of 'regional incidents' when many parties are at least temporarily impaired in addition to the apparently intended victim.

"Earlier this year an attack on one or more targets in Amsterdam, the Netherlands, affected routes across most of Europe for four to five hours. Similar events are occurring somewhere around the industrialized world every quarter," notes Carpenter.

"These attacks have reportedly been targeted against eCommerce sites, but have often had the effect of 'blanketing' the available bandwidth and affecting a larger population of uninvolved websites and providers."

This growing 'joined-up' dimension of DDoS activity is one that organizations such as the European Union (E.U.) are monitoring. In October 2012, hundreds of cyber security experts from across the E.U. tested their readiness to combat cyber attacks in a day-long simulation dubbed the *Cyber Europe 2012* exercise.

In all, some 400 experts from major financial institutions, communications companies, internet service providers and local and national governments across Europe faced more than 1,200 separate cyber incidents (including more than 30,000 emails) during a simulated DDoS campaign.

The exercise tested how organizations would respond and cooperate in the event of sustained attacks against the public websites and computer systems of major European banks. The E.U. believes that, if real, such an attack would cause massive disruption for millions of citizens and businesses across Europe, and millions of euros' worth of damage to the E.U.'s economy.

"This is the first time banks and Internet companies have been part of an E.U.-wide, cyber-attack exercise," said European Commission's Vice President, Neelie Kroes.

"This cooperation is essential given the growing scale and sophistication of cyber attacks. Working together at European level to keep the Internet and other essential infrastructures running is what today's exercise is all about."

DDoS democratized?

Fears that the DDoS threat is getting more pervasive and more complex are perhaps borne out by the conclusions of the seventh *Annual Worldwide Infrastructure Security Report*[1] published in February 2012 by network security specialist Arbor

Networks. This report suggests that, whereas financial motivations used to be among the top drivers behind attacks, today ideologically-motivated 'hacktivism' is the single most readily-identified motivation behind DDoS activity.

Arbor Networks argues that, in the current environment, any business can become a target of an attack and, given the plethora of readily available DDoS attack tools, anyone can launch one. This represents a sea-change for the risk assessment model for network operators and their customers.

"What we saw in 2011 was the democratization of DDoS. Any enterprise operating online – which means just about any type and size of organization – can become a target, because of who they are, what they sell, who they partner with or for any other real or perceived affiliations," reports Roland Dobbins, Arbor Networks Solutions Architect for Asia-Pacific, and the primary author of this year's report.

He adds, "Furthermore, the explosion of inexpensive and readily-accessible attack tools is enabling anyone to carry out DDoS attacks. This has profound implications for the threat landscape, risk profile, network architecture and security deployments of Internet operators and Internet-connected enterprises."

Denying the deniers

There is much organizations can do to defend against DDoS attacks, even the most sophisticated: both prevention and a plan for remediation are necessary. "Prevention is achieved by ensuring adequate overcapacity for requests, alternate routes, and null-routing [providing a network route – routing table entry – that goes nowhere], or equivalent technologies, like those of Cisco or Sooth," Carpenter explains.

"Any enterprise operating online – which means just about any type and size of organization – can become a target, because of who they are, what they sell, who they partner with or for any other real or perceived affiliations."

"Remediation includes not just additional capacity for requests, but may also require third-party filtering or scrubbing services like Prolexic [whereby traffic passes through a 'cleaning' or a 'scrubbing center' via various methods such as proxies, tunnels or even a direct circuit], as well as active defenses against the 'real' exploits often hidden by a DDoS attack against a target of intent, such as the fourth generation DLP [Data Loss Prevention] from Check Point," he adds.

Meantime, some key performance indicators (KPIs) for evaluating the performance of DDoS defenses have been developed by the TM Forum's Cyber Ops Metrics Project Team and are proposing in its forthcoming *Quick Start Guide: DDoS*[2] publication. Among them are:

- Measuring spare capacity, and specifically, how many more sessions could be supported than are used? This can involve third-party assistance to sort false from legitimate transactions, and to prevent all or some of the spurious requests from consuming the protected network's resources, using techniques including (but not limited to) null-routing, filtering (not allowing packets to pass through the firewall unless they match the established rule set) and scrubbing.
- Assessing deflection percentage, meaning that for an attack saturating the available spare capacity, establishing what percentage of spurious requests can technically be 'negated' through null-routing or equivalent mechanisms?
- Looking at the mitigation percentage, that is, the capacity of systems to identify spurious requests and prevent them from consuming (some or all of the) resources of the protected network(s).

Carpenter points out that best practices for contracting across an entire supply base is the most vital work TM Forum has done this area.

This is because it focuses on practical business preparations and responses to DDoS and related exploits, not just tweaking 'white-listing' (that is maintaining records of legitimate parties who have particular privileges, service, mobility, access or recognition) or other mechanical security techniques.

They are all ultimately limited by the capacity the victim is willing to maintain or contract as needed. He adds that the best prevention is achieved by collaboration with law enforcement to provide data to identify and remove hackers from the environment.

So what for the future of DDoS defenses? Carpenter places some store on the active detection and triangulation of attackers by carriers, service providers and even major websites with multiple points of presence.

Beyond this there is the active sharing of that information, as well as the 'impact analysis' of the effect the various DDoS prevention and remediation methods available can have on 'bystanders', to prevent collateral damage that might occur if only the benefit to the attacked network is considered.

[1]See www.arbornetworks.com/research/infrastructure-security-report for more information
[2]All of the Cyber Security best practices will be downloadable from our download center: www.tmforum.org/DownloadCenter/14250/home.html. The proposed publication date is alongside the Frameworx 13 release in May 2013.

COUNTERING HUMAN ERROR AND MALICE TO **PROTECT YOUR ORGANIZATION**

Only too often human factors, rather than technological deficiencies, are the root cause of compromised security. If anything, the focus on human fallibility, curiosity, frustration, discontent, misbehavior or criminality in the context of cyber security breaches has intensified, in line with the number of new opportunities arising from cloud computing, bring your own device and enterprise social networking, among other innovations. Here we look at the scope of the threat and some pragmatic steps to defend against it.

FOR THE ORGANIZATIONS who are victims, successful breaches of and interference with modern IT and networking systems can have a potentially huge costs. These are in terms of financial loss, destruction of brand and reputation, and damage to sovereign national interests.

Not surprisingly, organizations all over the world are making major investments (see panel) made to improve the technologies and IT systems that can be used to warn of, protect against, and recover from these eventualities.

The effect the human factor has on security is highlighted in the *10th Annual Information Security Trends* study[1], carried out by the Computing Technology Industry Association (CompTIA) and published in November 2012.

In it, the majority of companies surveyed acknowledge that human error is a contributory cause of security breaches, just as they have in the previous nine years of the study.

"Spending on security products shows no signs of abating, but a comprehensive security solution also must focus on the end users," states CompTIA's Director, Technology Analysis, Seth Robinson. "It boils down to policies, processes and people; making every user aware of their responsibilities for security."

"The human element is one of the most important elements in preventing security violations and breaches. Aware and well trained staff are much better able to recognize and prevent threats," agrees Alex Hamerstone, Compliance Manager at the native, cloud-based mobile field service management software specialist, TOA Technologies. "Many attacks require action on the part of the victim, and when users are educated there is less chance that they will do something to compromise their organization."

In this context, human factors refer to the elements of information security which are dependent upon people following security best practices. Employees with access to systems and data are generally the most vulnerable aspect of information security.

People problems on the rise

If anything, the focus on potential human fallibility, curiosity, frustration,

The scale of the problem

Some idea of the scale of the problem of security breaches can be gleaned from the response to it, in terms of the various means of trying to defend against it. For instance, Gartner estimates that revenue from unified threat management products and solutions reached $1.2 billion worldwide in 2011.

In addition, Global Industry Analysts reckon that global smartphone security software could be worth $2.99 billion in 2017, while MarketsandMarkets forecasts that the overall cyber security industry could be worth $120.1 billion by 2017, growing at a compound annual growth rate of 11.3 percent from 2012.

discontent, misbehavior or criminality in the context of cyber security breaches has intensified in recent years.

The introduction and growing adoption of technologies and innovations such as cloud computing, bring your own device (BYOD) mobile use and enterprise social networking have all involved surrendering varying degrees of centralized control and/or visibility of workforce activity, in the process elevating the importance of being able to manage the human elements of cyber security.

With cloud computing, an organization's data can be handled at one remove from its own workforce, a circumstance that forces prudent cloud clients to pay closer attention to who has access to that data.

The use of unauthorized mobile apps, and the accidental or deliberate introduction of malware, can more readily occur where the practice of BYOD is implemented in place of company-supplied technology.

"Because BYOD often means that it is more difficult to technically enforce company policy on devices, there is more reliance on the user knowing how to stay secure," remarks Hamerstone.

"Social networking is a great way for attackers to gather intelligence needed for a successful attack. Information truly is power, and social networking allows employees to share a great deal of information," he adds. "This information can be very valuable for social engineering attacks such as spear phishing. An educated user is far less likely to inappropriately share sensitive information or fall victim to social engineering."

For example, having gathered information from social networking sites about as senior executive's role in an organization, the criminal sends them a tailor-made email that they are likely to read and open the attachment, which might look like a spreadsheet if the target is the CFO, for instance.

Robinson equates the trend for users gaining more responsibility for their own technology with the human element becoming more and more important. "But many organizations are not sure what to do about it," he says.

"The way they've thought about security in the past is to purchase a firewall or antivirus software or other product. But there's not a product that can help with end-user awareness. It really requires a commitment to training and education."

As well as training and awareness, Hamerstone also points out arrangements whereby employees only have access to data they need to do their work, which minimizes the amount of data lost if there is a successful cyber attack.

Measuring success

The overall goal of security concerned with the human factor is to enable adherence to and enforcement of security policy where technical controls alone cannot deliver compliance and enforcement.

As noted in TM Forum's *Quick Start Guide: Human Factors*[2], in most situations it is extremely difficult to work out, with any accuracy, the effective the measures are which are designed to guard against human errors and malice.

Also, the assessment needs to be reinforced by people being told and shown what to do to protect systems and data, and their compliance with processes enforced. "Even the best security rules are useless if they are not followed," observes Hamerstone.

The TM Forum *Quick Start Guide* identified six core key performance indicators around security and human factors. As with all the *Quick Start Guides* referred to in this publication, the aim of the guidance is to identify the measures that will have the greatest impact.

- The percentage of employees who receive background examinations and the depth of such examinations.
- The percentage of employees who receive security awareness training on being hired.
- The percentage of employees whose training is repeated and updated, and at what intervals.
- The scores and pass rates of security-related training exams and how those who don't do sufficiently well are handled.
- The results of internal and third party audits of compliance with policy and procedure.
- The results of social engineering assessments and what happens when the results are not good enough.

The *Guide* also suggests a number of possible examples of what it considers 'commercially reasonable' terms around humans and security when drawing up or agreeing Service Level Agreements (SLAs) between partners. They include all employees receiving commercially reasonable background screens for their country; undergoing security training before working on customer data or support; and taking a security refresher course at least annually.

In addition, any employee failing security training twice will be removed from customer support, and contractors will provide an annual compliance and audit report certified by third parties. Finally, social engineering penetration testing will be performed at the same interval as technical penetration testing (quarterly) and any exceptions this control will be reported.

The authors' recommended use of this particular *Quick Start Guide* is as "…a minimum sanity check for the human factors security of any organization." The publication concludes that if an organization has not addressed the minimum considerations outlined, it may be exposed to one or more of the most common threat vectors for security in the world today.

[1]See www.comptia.org/news/pressreleases/12-11-14/Employee-Empowering_Technologies_Raise_Security_Stakes_for_Organizations_New_CompTIA_Study_Reveals.aspx for more information.
[2]*Quick Start Guides* will be published alongside the Frameworx 13 release in May 2013.

SECURING SERVERS IS **THE KEY TO SAFER DATA**

Some 97 percent of all data record breaches in large organizations involve a server being hacked, and the trend seems to be getting more prevalent. The good news is that relatively simple measures would deter most attackers, who generally search for weaknesses to exploit (in 79 percent of cases) rather than deliberately target particular enterprises. Either way, TM Forum's Collaboration Community is working to develop metrics to help organizations assess and improve their servers' security.

THE ACUTE IMPORTANCE of securing servers was highlighted in the 2012 Data Breach Investigations Report (DBIR)[1], complied and published by Verizon. It found that 64 percent of all data breaches and 94 percent of all data records breached involved servers, up 18 percent since the previous study two years earlier. For larger organizations, these figures were higher, at 68 and 97 percent respectively.

The study comments, "It's really not surprising that servers seem to have a lock on first place when it comes to the types of assets impacted by data breaches."

It points out that successfully hacking a server is highly likely to yield a far bigger quantity of data than any other asset.

Users' devices also store and process information too and are typically highly mobile, less restricted and controlled by the users. Consequently, they are frequently implicated in data breaches in some form.

Although data is stolen from them, more often they act as a gateway into an organization's IT, from which the criminal launches the main attack.

For larger organizations in particular, this often involves installing a keylogger on a laptop or PC to steal a person's username and password to access an internal application server.

The report also found that criminals' choice of target is based more on opportunity (79 percent) than choice; that is most victims were selected because hackers found a weakness that could be exploited – and often easily – rather than because they were chosen specifically.

However, this not always the case, as was highlighted on November 28, 2012 when a previously unknown group, Parastoo, hacked the UN's International Atomic Energy Agency (IAEA) via a server that was no longer in use. The hackers stole and published contact details of 100 nuclear experts on their website, asking them to sign a petition for the IAEA to investigate Israel's alleged nuclear program. The IAEA is investigating Iran's nuclear activities.

Whatever the motivation, securing servers is essential for all types of organization. Perhaps the most encouraging aspect is that, according to the DBIR 2012, 96 percent of attacks were not highly difficult to execute, implying that their prevention would not be too difficult – more a question of getting basic precautions and measures in place and updated.

Developing best practice

TM Forum has started working on cyber operations metrics to secure servers. It is aiming to publish its work in the form of a *Quick Start Guide* during 2013, offering key performance indicators so that our member organizations can assess and improve their servers' security.

"TM Forum has started working on cyber operations metrics to secure servers. It is aiming to publish its work in the form of a *Quick Start Guide* during 2013."

[1]The study is conducted by Verizon's RISK Team in cooperation with the Australian Federal Police, the Dutch National High Tech Crime Unit, Irish Report & Information Security Service, Police Central e-Crime Unit, and the United State Secret Service. For more information, please go to www.verizonbusiness.com/about/events/2012dbir/

MEASURING THE EFFECTIVENESS OF SECURITY IN THE SUPPLY CHAIN

In December 2012, a team championed by the Defence Science & Technology Laboratory (DSTL), an agency of the U.K.'s MoD, demonstrated how metrics could be used to measure the effectiveness of cyber security across a supply chain. CA Technologies, McAfee and Sooth Technology collaborated to develop a solution concerned with measuring the security of patch management across a supply chain as a first step in exploring this unusual, but increasingly important aspect.

MEASURING THE effectiveness of security is an interesting area because cyber defense usually focuses on what's gone wrong and its impact. "The flaw in thinking like this is that you're not looking at what works, how well it works and why, beyond the fact nothing's gone wrong with it," explains Luke Forsyth, Vice President, Security Services, EMEA, CA Technologies.

Yet this is hugely important. Forsyth continues, "We check the financial health of our suppliers to make sure they're not going to go broke in the foreseeable future and we check they've got the right kind of insurance in place, such as covering liabilities, but a cyber attack could stop a supplier operating just as much as having no money in the bank."

A lack of preparedness to deal with a cyber attack could have catastrophic consequences for a supplier's customers. Forsyth says, "Take a telco and a water company. If a telco is without water for an hour, the situation becomes acute because of sanitation problems and people needing to drink, and the telco has to evacuate the building.

"In turn, the water company needs communications to function, and the telco and the water company both rely heavily on diesel for transport and their reserve power supply. So all parties should know how well the other two are prepared. This is a massive business assurance issue across them all and is what's known as the nested supply chain problem."

TM Forum's Catalyst project (see panel on page 20), *Making security measurable: Define, contract and implement key performance indicators to prevent threats, end-to-end, in the supply chain* is a contribution to the ongoing work, by many organizations around the world (including the Global Economic Forum, the European Union through its Digital Agenda, Australian authorities and the U.K.'s DSTL) to address this and related cyber chain problems.

As Forsyth observes, "We need to work out ways of handling centralized cyber assurance data to ensure you don't have dangerous problems arising through inefficiencies, including huge duplication of effort and not using the data we have nearly as well as we could."

The group within TM Forum that has been working on cyber operations metrics[1] for over a year chose patch management as a first target for several reasons. For one thing, it is one of the biggest vulnerabilities in multi-partner networks today (hence the Forum's focus on it, see page 10).

As Iain Lobban, Director of British signals intelligence and information security organization GCHQ, says, "If government departments observed basic network security disciplines, such as keeping patches up to date, combined with the necessary attention to personnel security, their online networks would be much safer." This also applies to corporations and their suppliers. Assuring the confidentiality and integrity of those supplier networks is the key to resilient service delivery during a cyber crisis.

Also as Forsyth points out, "It is also one of the areas that is easier to automate for cyber metrics and also one that is easier to measure. The Catalyst was a conceptual idea of how things might be done, with three vendors showing how their solutions could look. It would be a very different issue dealing with 300 Fortune 1000 companies, say, and there is lots more work to do."

The scenario for the Catalyst project was a global corporation fulfilling consumer and government contracts through a diverse supply chain.

[1]Watch a webinar on the CyberOps Metrics project here: www.tmforum.org/UpcomingWebinars/2704/home.html#TRCWebinars/Link49768

ID	Business Unit	KPIs
1	Configuration Management	Time to apply patches/Time unpatched
2	Configuration Management	Completeness of patching across and on devices
3	Security	Criticality of deviation from patching standards
4	Security	Audited degree of systems susceptibility
5	Security	After-patch vulnerabilities
6	Architecture	Number of patches needed

Competition for government contracts and increasing dependence upon outsourced suppliers means the company must ensure cyber risk management techniques are applied throughout the supply chain. The integrity of the suppliers' networks must be measured to ascertain their level of cyber-readiness.

The Catalyst demonstrated a quantitative method, based on key performance indicators (KPIs) that enabled identification of problems between supply chain partners. The KPIs in the demonstration were developed for the *CyberOps Metrics Quick Start Guide: Patch Management*, which is available free to all employees of TM Forum member organizations by registering on the website (see page 10 for details). Having defined KPIs to enable the measurement of patch management, organizations are better able to draw up contracts with new levels of quantitative and specific detail, adding a new layer of accountability.

The patch management KPIs used in the Catalyst project are shown in the table above:

The example service level agreement[2] (SLA) used described the control requirements for critical systems, and the method and frequency of the measurement. An independently managed service provider monitored the cyber readiness of the supply chain, using automated assessment, analysis and visualization tools.

Applying common cyber risk management techniques, like patch management, across the supply chain delivers the following benefits:

- **Identifying the real business impact** – the expanding threat landscape has shortened the decision cycle so organizations need dynamic, continuous visibility of cyber risks linked to business processes.
- **Confidence in government** – public eServices are critical to secure society and confidence in government and demonstrating and measuring the security controls in place are critical for governments to show due diligence against cyber risks.
- **Competitive advantage** – businesses that can measure the security of their supply chain can show they are safeguarding against risk, which will make them more attractive to customers as a partner.

The security metrics used in this Catalyst project could be integrated into TM Forum's Business Metrics and Scaffold[3] work, while more Catalysts are under discussion to explore other areas to which the cyber operations metrics could be applied.

Forsyth comments, "One of the areas I'd like to see more work on is correlating information on anomalies across an organization. Small individual changes – the phone bill has gone up, more light bulbs are blowing, power consumption is a bit higher – don't look malicious individually, but collectively they could be signs of an advanced, persistent threat."

He concludes, "After all, such sustained attacks are deliberately low level to avoid detection and who will spot lots of very small fluctuations in so many different, apparently unconnected places? It's definitely a key area."

[2]TM Forum' *Service Level Agreement Management Handbook* (GB917) is available free to all employees of our member organizations who register on our website from www.tmforum.org/GB917SLAManagementv3.1
[3]The latest edition of the Business Benchmarking Metrics Scaffold (GB935) is available free to all employees of our member organizations who register on our website from www.tmforum.org/GB935businessbenchmarking

What are TM Forum Catalyst projects?

TM Forum Catalysts are short-term, collaborative projects which strive to create solutions for critical industry operational and systems challenges, as defined by different types of service providers, such as cable companies, defense agencies, enterprise IT departments and others.

The projects last between three and six months and their culmination is a live demonstration at one of TM Forum's Management World events. They are based on the Forum's Frameworx suite of standards-based tools and best practices (see page 21) and typically feed their work back into the Forum's unique Collaboration Community (which has some 65,000 active participants working on a wide range of goals) to extend and enhance those tools and best practices for the good of all TM Forum's members and the industries they work in.

Contact Megan Lunde, Catalyst Program Project Manager, TM Forum, for more information, including how to get involved, on mlunde@tmforum.org

EMBEDDING SECURITY IN FRAMEWORX

The importance of cyber security is recognized by TM Forum and has been embedded in Forum's Frameworx suite of standards-based tools and best practices. Here we look at how Frameworx can help organizations – from those in defense to digital service providers of all kinds – protect themselves, their partners, suppliers and customers.

FRAMEWORX IS DESIGNED as a blueprint for efficient business operations.

It was developed and is constantly evolved by TM Forum's unique Collaboration Community, which has some 65,000 individuals from our member organizations working within it, to meet the constantly changing needs of many business sectors. They include communications, digital service providers, cable, defense, utilities, and all sorts of enterprises.

Frameworx is free and exclusive to TM Forum's members, and helps them assess and optimize performance using a proven, service-oriented approach to operations and integration. Frameworx helps members:

- Innovate and reduce time-to-market with streamlined, end-to-end service management.
- Create, deliver and manage enterprise-grade services across multi-partner value-chains.
- Improve customer experience and retention using proven processes, metrics and maturity models.
- Optimize business processes to deliver highly efficient operations.
- Reduce IT systems integration costs and risk through standardized interfaces and a common information model.
- Gain independence and confidence in procurement choices through conformance certification and procurement guides.
- Gain clarity by providing a common, industry-standard language for processes, information and applications.

The latest release, Frameworx 12.5, was published in December 2012 and added considerably to security features. It builds on previous releases and bridges towards future ones, across all four components of Frameworx; a brief outline of each is given below.

Information Framework (SID)

The management of services, customer experience, networks and enterprise management functions demands consistency of data across an enterprise.

The Information Framework provides a comprehensive, industry-agreed, structured set of definitions for the information that flows through an enterprise and between service providers and their business partners.

It is supported by off-the-shelf tools for implementing in software, reducing the time and effort needed to create standardized integration points.

Business Process Framework (eTOM)

The Business Process Framework defines a comprehensive set of efficient, clear and effective business processes critical to running any kind of service provider's business, at the lowest possible cost.

It provides a multi-layered view which starts with primary organizational functions and drills down to thousands of process details, in four levels. It is strongly aligned with ITIL and supported by off-the-shelf tools to provide a catalog of business processes, which can be implemented.

They include users' guides and sample process flows to help streamline processes within an enterprise and across partners in a value chain.

Application Framework (TAM)

Understanding how your business processes are implemented in software systems is essential.

This Framework provides a model for grouping processes and their associated information into recognizable applications that span the service provider's operations, business and enterprise management functions.

It provides a common language and identification scheme between buyer and supplier for all application areas. It helps in the design of enterprise architecture through a better understanding of systems.

Integration Framework

This Framework provides direction on how operational processes can be automated using standardized information definitions from the Information Framework to define standardized Service Oriented Architecture (SOA)-based management systems.

It also provides an automated means of creating standardized interfaces and using them to integrate applications within the enterprise and with partners.

Security in Frameworx

Security was first embedded in Frameworx in 2010 in the form of a Network Defense (NetD) model from the U.S.'s National Security Agency (NSA), including an implementation guide and definition dictionary.

It gave TM Forum valuable insights on how to model threats, incidents, events, assets and vulnerabilities. The model was based on National Institute of Standards and Technology's (NIST) security content and automation protocol standard (SCAP) and integrated into the Information Framework.

NIST released an updated version of SCAP, 1.2, which supports three kinds of scoring to calculate the seriousness of a vulnerability. They cover: common configuration, common vulnerability; and common misuse. TM Forum has extended the enterprise security Aggregate Business Entity in Frameworx 12.5. published in December 2012, to include them.

Frameworx 12.5 saw other important additions too – most notably in the area of assuring security. The cyber operations team looked at research and best practices from a variety of respected sources – including NIST, NSA, the SANS Institute and Australian Defence Signals Directorate (DSD) – to establish how best to proceed.

They found that a common theme was the Pareto Principle, which is that roughly 80 percent of the effects come from 20 percent of causes. So the team set out to answer the question which 20 percent of measures would deliver 80 percent or more greater improvement?

Patch management, a subset of configuration management which is vital to preventive security, was chosen as the first area to work on because it cropped up so frequently, typically due to organizations deploying operating systems out of the box without hardening and modifying them.

The next four most critical areas were identified as being; human factors, mobile device management, distributed denial of service attacks (DDoS) and server security management.

The team set out to define key performance indicators (KPIs) for each, which could be instrumented and implemented easily and systematically, across the supply chain with nested and industrial-scale connectivity, not just a simple, cascaded supply chain.

They are available in the form of Quick Start Packs, which also offer guidance on best practice, and are already available free to TM Forum member organizations for patch management, human factors and mobile device management.

The Packs for DDoS and securing servers are scheduled to be released alongside Frameworx 13 in May 2013.

Use cases

Earlier in 2012 the security management project developed three themed security use cases; penetration attack, distributed denial of service attack (DDoS) and application abuse/misuse.

From Frameworx 12.0, released in May 2012, the team wrote a technical report (available free to member as TR1731), which includes the process steps involved for each across all operational states.

From this work the team identified Level 3 processes for the Business Process Framework which were included in Frameworx 12.0. The team took two of those use cases – the penetration attack and DDoS – for Frameworx 12.5, mapping their processes to those in the Business Process Framework, which was added to and definitions amended.

The work was published as an annex to TR173 alongside Frameworx 12.5. The next step is to develop process flows and Quick Start Packs for each of the use cases.

Technology taxonomy

Alongside these efforts, the security project team was looking at ways to develop a better taxonomy for mapping security applications to the Application Framework (TAM) and became aware of an IT security industry taxonomy developed and managed by the Security Innovation Network (SINET). Its mission is to advance innovation and enable global collaboration across public and private sectors to defeat cyber security threats.

The taxonomy depicts the spectrum of cyber security technologies available commercially and has been in use for over a decade. It changes constantly to reflect the dynamic nature of the security industry and maps over 1,000 products, arranged into 17 categories and 150 sub-categories.

The organizations signed a Memorandum of Understanding in 2012 for the Forum to evaluate the SINET taxonomy with the objective of factoring these topics into the Application Framework.

Importance of interfaces

The Enterprise Security Project operates within the Forum's interface program and offers three key interfaces to the Forum's members, which are free to download, but at different stages of maturity and part of the Integration Framework. They are interfaces for Operator User Management, Single Sign-On/Off and Security Compliance Audit Automation.

[1]See www.tmforum.org/securitymgmt/downloads

tmforum

Everything that can be digital will be.

We've seen the future. And it's digital. In just ten years, the way we communicate, consume information and entertainment has been changed forever. And that's just the start.

The Digital Revolution is transforming our personal and professional lives. We demand simplicity, but the complexity behind our interconnected digital lives is only growing.

TM Forum's Digital Services Initiative focuses on overcoming the end-end management challenges of complex digital services, enabling an open, vibrant digital economy.

There are five core principles of the Initiative:

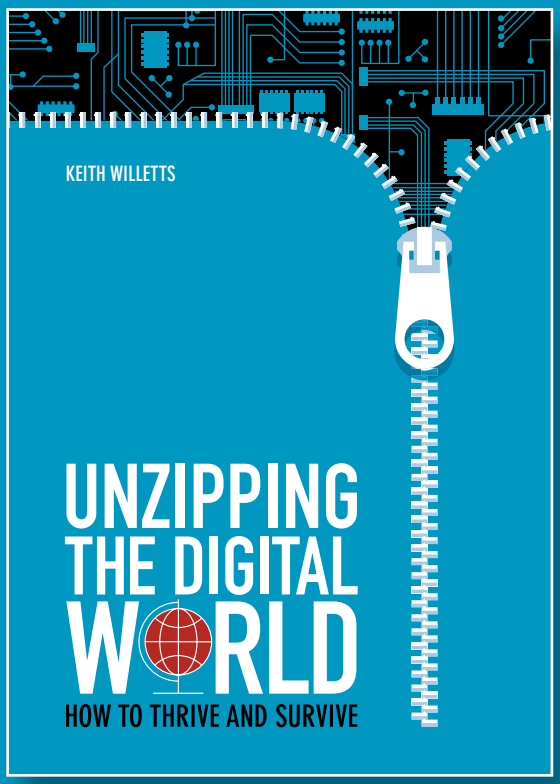
OPEN	Enable a virbant, open digital services ecosystem
INFORM	Provide market intelligence and research
INNOVATE	Support rapid and successful innovation
ACCELERATE	Enable efficient and effective service delivery
OPTIMIZE	Automate and optimize with tools and best practices

For more information on the TM Forum Digital Initiative visit www.tmforum.org/digital

UNZIPPING THE DIGITAL WORLD

A NEW BOOK BY KEITH WILLETTS

AUTHOR, TM FORUM CO-FOUNDER AND CHAIRMAN, COMMUNICATIONS WEEK TOP 25 INDUSTRY VISIONARY, BRITISH COMPUTER SOCIETY AND BT GOLD MEDAL AWARD WINNER.



A 'digital tsunami' is feeding on itself driven by cloud, mobile broadband, smart devices and a mushrooming 'internet of things' enabling every sector of every business to rethink how business is done - almost anything that can be digital will be. Willetts unzips the market with a 'no holds barred' picture of what today's giants need to do to thrive and survive in the rapidly expanding digital world and presents a practical series of steps on how to exploit the massive opportunities the digital economy presents.

"TWO THUMBS UP! THE FUTURE FOR OPERATORS WILL COME FROM EXPLOITING NEW SOURCES OF REVENUE IN THE DIGITAL WORLD WHICH ARE SO WELL SET OUT AND EXPLORED IN THIS BOOK."

PAUL BERRIMAN, CHIEF TECHNOLOGY OFFICER, PCCW

www.tmforum.org/unzippingthedigitalworld