Corporate Treasurers Council®

CTC GUIDE

Cybersecurity: Setting a Cyberrisk Management Strategy

Supported by

MARSH & McLENNAN COMPANIES

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

WHAT'S THE RIGHT WAY TO MANAGE RISK? THE SMARTEST PATH TO GROWTH? THE BEST WAY TO ENGAGE YOUR PEOPLE?

When it comes to risk, strategy, and human capital, clients in more than 130 countries depend on us to help them answer the hard questions. Together, we work to solve complex problems, seize opportunities, and drive growth.

We are Marsh & McLennan Companies, a global professional services firm whose deep expertise and commitment to lasting partnerships protect and advance our clients' vital assets: their people, their capital, their strategy.

To learn more about us and our market-leading brands, visit MMC.com.

MARSH GUY CARPENTER MERCER OLIVER WYMAN

Corporate Treasurers Council®

CTC GUIDE

Cybersecurity: Setting a Cyberrisk Management Strategy

Contents

Cybersecurity: Setting a Cyberrisk Management Strategy

Executive Summary

The Washington D.C.-based Center for Strategic and International Studies has estimated that cybercrime costs the global economy USD 445 billion a year. The *2015 AFP Risk Survey* found that 34% of companies had been subjected to a cyberattack in the last 18 months. For most corporate leaders, the well-publicized cybersecurity breach at Sony that took place in late 2014 was simply the latest instance of a type of crime that has risen to the top of their agendas.

This guide is designed to help organizations establish a cybersecurity management strategy and policy, both at corporate level and within the treasury department. The guide suggests and explains a three-part approach to establishing and implementing a cyberrisk management strategy: identify data at risk, value this data, and manage the risk appropriately.

When managing cybersecurity, companies should prioritize the use of resources to protect the most valuable and business-critical data. The guide explains when and how to use cyberrisk insurance. Finally, underpinning the guide is an assumption that it is impossible to eliminate all risk of a cyberbreach. With this in mind, the guide concludes with suggestions on how to plan a response to the likely data breach.

Return to Contents

What is the Cyberthreat?

Seemingly every day there is a new report of a high-profile security breach at a major national or multinational corporation. The sources vary from alleged state-sponsored hacking through to breaches caused by employee error. These reported cases are the tip of the iceberg: for all the cases that are made public, there are many others which remain below the radar. Whatever the reason, each affected corporation faces a hit to its reputation and a degree of additional cost. At a minimum, companies have to finance an internal inquiry to establish how a breach took place and then pay for any recommended measures, such as investing in more training for employees. At the other extreme, regulators may require companies affected by a breach to pay significant sums in compensation. The highly publicized security breach at Sony highlights just how far the implications can extend. Given the size of the events and the potential impact on corporations of all sizes, managing cybersecurity has risen to the top of most corporate agendas.

Just as importantly, corporate strategists have realized that cyber protection is not as simple as putting in place a strong firewall. Put simply, firewalls have never been (and can never be) completely secure. Moreover, tight firewalls are counterproductive. In today's interconnected world, corporations need to be able to communicate openly with third parties: companies make supplier payments electronically, for example, and customers, both B2B and B2C, increasingly expect to be able to purchase goods online.

This means companies are faced with the challenge of managing cyberrisk in an ever more complex environment, while retaining the ability to communicate effectively with customers, suppliers and other trusted third parties.

How can treasurers help to manage cyberrisk?

Within this context, there are two roles for a corporate treasurer to play when seeking to manage cyberrisk.

First, the treasurer is well placed to help the company develop a group-wide strategy for managing cyberrisk. In particular, treasurers have well-developed risk management skills. They will be able to apply their asset valuation skills to identify the assets within the organization which require protection. Treasurers also have project management skills and an understanding of the structure of their organizations: both are needed to coordinate a group-wide approach to cyberrisk management.

The second part of the treasurer's role is to manage the cyberrisks that are directly relevant to the treasury department's day-to-day activities. Treasury departments have been investing in technology to be able to automate processes and achieve efficiencies. Yet these efficiencies require organizations to be more connected to third parties, via the internet and other connections, resulting in a much greater exposure to cyberrisk. Treasurers need to manage cyberrisks associated with most of their core activities: payment processing, liquidity management (including the operation of in-house banks), supply chain management and the use of any outsourced services, including treasury management systems and other solutions offered as a Software as a Service (SaaS).

Setting a cyberrisk management strategy

This guide examines both elements of a treasurer's role in managing cyberrisk. The underlying principles are the same, whether the risk is being managed at the corporate or department level. In both cases, it is appropriate to take a three-step approach to developing a cyberrisk management strategy:

1. Understand the nature of data which is at risk

   Before setting any strategy, the treasurer (together with other appropriate colleagues) has to have a clear knowledge and understanding of the scope of data, information and activities which is potentially at risk.

2. Value the data at risk

   Once the scope is understood, the treasurer will help to place a value on all data. Both assets at risk (such as the long-term value of intellectual property) and potential liabilities (for example, likely compensation payments) will need to be quantified.

Return to Contents

3. Take action to manage the data at risk

With a clear value of the data, the treasurer can then help the group to prioritize the use of resources to manage cyberrisk effectively. Within this process, there are essentially three tasks:

- Protect the most valuable data

  Companies should dedicate their scarce resources to protecting the most valuable data. This is likely to include data which is central to the financial viability of the organization, and will include core intellectual property. Protection is likely to be achieved via a series of measures and controls.

- Manage the remaining risk through insurance and self-insurance

  Irrespective of how much is spent protecting the most valuable data, there is still a chance that security will be breached. It may be possible to use insurance to cover this remaining risk. For example, insurance is often appropriate as a protection against any requirement to pay financial compensation as a result of a data breach. However, it may not be possible, or financially appropriate, to insure against every potential loss.

- Adopt a plan should a data breach occur

  Finally, all organizations should expect a data breach to occur at some point. The challenge then becomes how best to respond to ensure any risk to reputation and any financial losses are minimized.

Ultimately, a corporation needs to be able to determine who should have access to each piece of its data, and have in place a process to protect it or a solution to be able to recover in the event of loss.

How to coordinate the development of a cybersecurity strategy

Aim for a collaborative process

To achieve the full picture of the value of group assets, a collaborative process must be established. There must be a group-wide committee or other structure tasked with setting and implementing the cyberrisk security strategy. This committee must take an enterprise-wide approach, and it may be appropriate to incorporate the cyberrisk security strategy into the wider enterprise-wide risk management policy. The key is for the committee to be inclusive from the earliest point, so that individuals within the company are able to share their particular concerns. The committee must also be able to coordinate input from all the relevant divisions and entities. Although this will be a significant challenge in multinational corporations operating in many jurisdictions around the world, it will still be a challenge in a company with activities primarily in the home market. Unlike many other group activities, it is not appropriate for a cyberrisk strategy to be conceived in terms of silos of internal activity.

Board-level support is required

This committee must have board-level approval and authorization to require all group divisions and entities to cooperate.

Ensure appropriate team membership

The committee's membership may vary over time once the initial strategy has been set and there is a movement towards implementation and ongoing review.

Aim for accountability

The committee must be under the named direction of one individual responsible to the board for the performance of this committee. That individual is unlikely to be anyone directly involved in IT, although it could be the director responsible for, among other things, IT.

In the following sections, we examine each step in the process of establishing a cyberrisk management strategy in detail.

Return to Contents

Sources of Cyberrisk

Understanding the nature of cyberrisk involves two elements. First, companies need to understand the types of individual and group which pose both specific and general threats to their cybersecurity. Second, companies need to understand the full range of information at risk within their organizations. These factors need to be evaluated on a group-wide basis and at the treasury department level too.

Who poses the threat?

The first stage of the strategy should be to try to understand the individuals and organizations that represent the greatest threat to cybersecurity. Companies will be affected differently, according to the nature of their business, their customers and suppliers, and the locations of their activities. Verizon's 2014 Data Breach Investigations Report analyzed security incidents over a ten-year period. It found that, for example, companies in the travel and hospitality sector were most likely to be affected by attacks on point-of-sale technologies, whereas retail companies were most likely to be affected by denial of service attacks.

Being aware of the most likely sources of cyberrisk will help to determine the most appropriate approaches to protecting the most valuable data. Because the nature and objectives of the individuals and groups launching attacks vary, the responses by organizations may need to vary too.

Internal threat

The primary threat comes from internal sources: current and former employees of corporations, including disgruntled former employees whose credentials have not been canceled.

The internal threat to cybersecurity should not be underestimated, for two reasons. First, because internal employees potentially have access to the full range of corporate information, there is a risk of significant loss if appropriate controls are not in place to manage individuals' access to data.

Second, evidence from law enforcement agencies suggests that, while cyber losses caused in this manner are not often publicized, they represent the most likely form of cyberattack. Security breaches can be deliberate: a disgruntled or blackmailed employee may decide to reveal or sell information to third parties. The chances of a breach can be reduced via improved training: the introduction of a USB pen drive or the failure to follow established procedures can allow malware into a company's systems. But, however comprehensive a company's training program is, some internal breaches are still likely to occur. For example, the volume of phishing emails means that some will inevitably be opened, and it remains very easy to copy third parties into internal emails accidentally, especially when using unfamiliar devices to communicate.

Specific attacks and general threats

External attacks from third parties are initiated on organizations for a variety of reasons, with certain types of attack more likely in some industries than others. For example, organizations may face specific attacks because of the type of business they do (pharmaceutical companies may be more susceptible to industrial espionage attacks, oil companies may attract environmental activists and retail companies may face threats at the point of sale). The nature of an organization's business partners may also result in certain specific threats: companies operating in the defense industry or with links to government may face threats from other governments.

As an indication, external threats arise from four main types of opponent:

Hackers

The first category of external attackers is IT-focused hackers. They are primarily motivated by the challenge of attacking corporate cyber defenses. If they are successful, they may highlight this by disrupting processes or otherwise publicizing the breach. There are also ethical hackers who work with organizations to improve their cybersecurity by trying to breach existing arrangements.

Activists

Rather than viewing the target as a challenge in itself, activists are motivated by causing disruption and/or

Return to Contents

embarrassment to a specific target (or target group). Activists often have environmental or other political reasons for targeting a particular company or category of companies. Their attacks are typically intended to make a campaigning point and may be directed at taking over websites or performing a denial of service attack so that the company cannot continue to operate normally. Energy companies, financial institutions, companies with links to particular political regimes and those in the defense/military industries are more likely to be susceptible to these types of attack.

Financial criminals (internal and external)

Financial criminals look to obtain protected data, often in the form of personal information such as customers' credit card details, then to sell that data into the black market. Phishing is an increasingly common way of seeking this data, although attacks may also be targeted at particular processes or systems. They can also be initiated internally by a dishonest employee providing access to systems or particular data sets to criminals for onward gain.

General attacks rely on weaknesses in internal systems or procedures to gain entry to the company systems. For example, phishing is successful when an employee inadvertently opens a corrupted email or other corrupt file. Employees can weaken security via the introduction of USB pen drives into the company network or by the use of personal computers when working remotely or from home. Companies should be wary of the use of cell phones and tablets to communicate with their systems. These can expose the company to a greater degree of cyberrisk simply because of the different levels of security in mobile protocols.

Intellectual property thieves

Finally, and most seriously, some individuals or organizations, including governments, launch attacks to try to obtain access to the target's intellectual property (IP). Such data may include core production information, such as formulae and production methods: the loss of control of this data may allow another company to produce the same items more cheaply, threatening the long-term future of the target. Third parties may also want access to negotiating positions and tender documents when bidding for contracts.

It is also possible for industrial espionage to be conducted by employees, either as a result of disgruntlement, as part of a transfer of employment (the employee brings confidential information with them), or as a result of some financial inducement (possibly including blackmail).

Understanding where threats may come from will help companies to manage the risk. That said, Verizon's analysis found that 75% of successful data breaches were not targeted at a specific individual or company, and that 78% of data breaches did not require any significant resources by the perpetrator. In other words, ensuring there is a good core set of security processes and procedures may significantly reduce the chance of a successful data breach. For example, setting clear protocols on the cancelation of credentials when someone leaves the company will help to reduce the threat posed by disgruntled employees. Improved training and clearer technology-use policies will help to reduce the likelihood of human error. Understanding the value of different data to third parties will also help to prioritize protection.

What is at risk?

Understanding the objectives of individuals and organizations posing a threat is only part of the equation. Companies also need to understand the full range of data and information which they hold and use, and to assess how and when the data is vulnerable. Companies need to protect physical and electronic data in two forms: when it is static (or at rest) on their systems, and when it is being communicated (or in flight), both internally and with third parties.

Data can be affected in three different ways:

1. Data can be stolen and sold to third parties or otherwise published. The impact will vary according to the nature of the data. The loss of customer information, such as credit card details, will result in a reputational loss and a consequent loss of sales, as well as possible regulatory fines and damages. The loss of core intellectual property may result in a third party being able to produce goods of the same quality for a lower cost.

Return to Contents

2. Data can be corrupted. Depending on circumstance, this could result in companies making decisions on the basis of incorrect data, or a manufacturing process producing sub-standard goods, exposing the company to longer-term financial loss.
3. Data communication can be halted or prevented. For example, company websites can be subjected to denial of service attacks, meaning customers cannot purchase goods online. Internal and external communications may also prevent data, which is essential to the normal running of the business, being sent and received from some or all parties, such as group entities, suppliers or banks.

When developing a company-wide cybersecurity policy, the team responsible needs to understand the complete range of data the company holds. Similarly the team needs to understand the scope of data held outside the organization (for example, with third parties including software partners and in the Cloud), and also when and how data is communicated externally. If this data is compromised in one way or another, there is the potential for a range of consequences.

To do this, the team needs to collate information from across the group. A checklist to help this process is provided at the end of this guide.

What are the key issues for treasurers to manage in the treasury department?

The challenge for treasurers over recent years has been to use the development of technology to automate processes and reduce operating costs (including headcount). However, this increased reliance on automation and straight-through processing also exposes the organization to a greater degree of cyberrisk. Cyberrisk is not simply the risk of systems being breached from outside the organization. There is also the risk of an internal breach where controls and limits are known, and can therefore be abused, and be difficult for audit to pick up.

As with the more general issues, fraud and human error remain the biggest risks within treasury departments. Human error when dealing can result in significant loss, especially if the approval processes are unclear or are not followed. With data flowing into and out of the treasury department, there is an ever-present risk of system corruption. For example, forecasting and positioning systems can foster errors, especially when estimates and actual data are confused. As more people gain access to treasury management platforms (often indirectly, when entering data into a forecasting module), there is more chance of both data corruption and malware being imported into the system.

As well as supporting the group to assess the data it holds, treasurers also need to understand the data they are responsible for within their own departments. Fundamentally, data falls into three categories: financial information held within the department, information collated from sources not directly under treasury control or from sources outside treasury responsibility, and communications with third parties, including banks, suppliers and customers.

Just as the group cybersecurity management team should identify all the data the company holds, so the treasurer should also perform a similar exercise at department level. The first step should be to understand both the type of data held and used and the systems through which that data passes.

- Internal systems

  There are a number of areas where internal systems represent a cybersecurity risk. In most cases, these are internal systems which are used to inform decisions, manage positions and reconcile transactions, and include treasury management systems, electronic banking systems, ERP systems and spreadsheets. Such systems vary significantly regarding their functionality, with some able to initiate and authorize a range of activities, include payments and investments, whereas others are primarily data repositories used to record activity.

  Data can be stored within some or all of these systems and might include information such as bank account balances, payment information, ledger entries and standard settlement instructions. There are two risks: first, that this data can become corrupted either as a result of deliberate action or because of a failure in the underlying software or user error. The challenge will then be to restore data, which will take at least some time and resource, depending on the

Return to Contents

nature of the breach, how long it has been between the breach and its discovery, and the type of backup services available from which to perform a restoration. The second risk is that the company may have been operating with misleading data. In a worst-case scenario this might result in the company being unable to meet its obligations, entering into unhelpful hedging transactions, or simply having cash in the wrong place.

Where data is collated from outside the treasury department, perhaps for cash positioning purposes, this may require individuals within the operating companies to have access to the treasury management platform. Controls should be in place in two key areas: first, operating companies should only have access to as much of the system as is necessary for them to perform their task. Second, any entered data should be subject to a reality check, so that data is interrogated on its merits.

Treasurers will also want to be wary when using spreadsheets, especially when they are used for payments as well as forecasting. Spreadsheets are inherently less secure than treasury management and ERP systems. Password protection can make them more secure, but data can become corrupted more easily, both within the spreadsheet and when data has to be entered into the accounting and other management software.

- Communication along the supply chain

  Supply chain finance solutions represent a significant risk, due to the widening scope of individuals and entities having access to a platform. Although any such scheme should include proper due diligence before it becomes operational and before entities are accepted into the program, and should incorporate good levels of control once in place, the treasurer of the company financing the scheme will not have the same audit access over the third parties which might be in place for group liquidity management structures.

- Communication with banks

  Although the controls are usually well established and good, there are risks associated with mobile data, in particular, and banks themselves are constantly being bombarded by hackers. All communications with banks are already subject to high-level controls, with SWIFT messages, for example, encrypted in flight.

  Most companies put in place good protections so that different individuals are responsible for initiating and then authorizing payments, for example. Access to systems is controlled via a range of different protocols, including the use of personal identifiers and activity limits embedded in the system.

  However, because of the level of protection offered in this environment, there is a risk of complacency. All protections can be breached, and treasurers will want to work to ensure that their internal protocols (such as their password policy and individual limits) remain relevant. This is particularly important after a change in personnel, to ensure previous permissions are canceled and that limits are set appropriate to new hires' expertise and experience.

- The use of outsourced services

  Treasurers will be concerned about the activities outsourced to third parties. These activities include investment management, especially the use of specialty fund managers, and the use of software solutions provided as Software as a Service (SaaS). SaaS has data and systems hosted remotely, so that companies must have a dedicated method of communicating to the systems. While some companies choose to host their treasury management systems on site, vendors are seeing increased demand for offsite hosting on the vendor's own servers (or outsourced servers managed under license on the vendor's behalf). Companies can choose to have a dedicated server at the vendor's location, with access via a dedicated line (on a VPN), or to share bandwidth and servers via a SaaS solution. The use of shared architecture does represent an additional risk which needs to be managed. This risk is magnified because of the value of transactions effected through the TMS.

As well as understanding the data for which the treasury department is responsible, the treasurer will also need to understand the system infrastructure and workflow, to minimize the risk of data corruption. Note that some data can feed straight into an ERP system, bypassing the treasury management platform. This might include

Return to Contents

vendor payments, where the accounts payable system is run through the ERP system. In all cases, the treasurer must understand how the treasury management system, especially the forecasting modules, captures data from other systems and collates data entered by other group entities. Without this knowledge, there is a very real risk that forecasts and actual positions will be inaccurate, resulting in inefficient decision-making in the treasury department and in potential loss.

Having a clear understanding of data

A process of establishing the full scope of data for which the company is responsible is essential in developing a cybersecurity policy. Without this understanding, the policy will be too limited in scope and will result in insufficient protections being implemented. More importantly, it could result in significant and serious loss, in the event of the inevitable cyberbreach.

The *2015 AFP Risk Survey*, supported by Marsh& McLennan Companies, (www.afponline.org/risksurvey/) found that the three most significant areas for concern with regard to **cyberrisk** were **reputational damage, loss of customer data, and loss of confidential personnel data**. Interestingly,companies which had experienced a cyberbreach were much more concerned about the loss of personnel data than companies which had not.

Return to Contents

Evaluating Cyberrisk

Having identified the full range of data, information and processes which are at risk, and the likely implications for the company should that data be corrupted, stolen or lost, the next step is to evaluate the actual value of the assets and the potential liabilities to the company.

Value assets and potential liabilities

The rationale for companies to identify all the assets they hold was discussed in the previous section. Naturally, the precise nature of these assets will vary significantly from company to company. The most common variations will be a function of corporate structure (where the company operates, where the company makes its decisions – centrally or locally – and the number of countries in which it operates) and the nature of the company's activities (mining companies will hold different data from pharmaceuticals, retail companies will hold different data from professional services companies).

The next step is to place a value on all these assets and work to understand the extent of any liabilities, should a breach occur. It is just as important to understand the extent of any liabilities should anything go wrong. Again, the extent of liabilities will vary quite significantly, depending on the nature of a company's activities and its customers and also the location of those customers. Insurance premiums to cover cyberrisk are highest in North America, especially the USA, because of the relatively high level of liability cover required.

The objective of this process is to be able to set a value for each set of assets at risk so that the team can prioritize its protection spend.[1]

Why value assets?

The purpose of placing a value on assets is to try to identify the business-critical data. This will not necessarily be core financial data or management information, especially in a publicly listed company. Although access to this data may give competitors an insight into the company's operations (and give them an advantage when bidding for new contracts), it should not result in the company's demise, even if it takes some time to restore any lost or corrupted data.

Raj Bector, Partner at Oliver Wyman:

> "There are a number of different techniques available to value the data held by the company with the results expressed in a number of different ways: for example, as revenue or shareholder value, or in terms of goodwill. However the calculation is made, the aim of the valuation is to identify the core assets which need protection."

Instead, business critical data is most likely to be intellectual property. Again, this will vary significantly, depending on the nature of the company's activities: it could be a pharmaceutical company's formulae; an automobile maker's manufacturing processes; or methodologies, in the case of business services companies. First, the company needs to understand fully where this business-critical data is located, who has access to it, and how and when it is transferred both within the group and to external parties.

The next stage is to try to quantify what would happen after different types of security event. These could include a simple loss of data (by deletion), a corruption of data (either by accident or on purpose), or the theft and onward sale or publication of data. Results can range from a short-term loss of production until activities can recommence, to the production of sub-standard items as a result of corrupted data (and the need to replace these goods), to the long-term failure of the company as competitors are able to undercut the company using the original plans.

The next stage is to try to value these assets, so that a clear view of the most valuable assets can be developed. The treasurer's expertise here is crucial, given the importance of valuing financial assets from a treasury perspective. Note that the valuation processes should consider both immediate losses and any consequent loss of sales and future sales. This can be difficult to

1. This value-based approach is explored in a paper written by David X Martin and Raj Bector of Oliver Wyman. It can be found here: www.olive-wyman.com/insights/publications/2014/jul/a-new-approach-to-cybersecurity.html.

Return to Contents

determine, partly because the consequential loss is difficult to evaluate.

The treasurer has to identify the best way to value the assets to the company as a whole. There are a number of choices:

- Value assets by the revenue they contribute to the company as a whole.
- Value assets by their contribution to overall shareholder value.
- Value assets, at least in part, by their contribution to goodwill.
- Value assets from an opportunity cost perspective by calculating the resource required to replace or repair any lost or corrupted data.

The primary objective of this exercise is to be able to prioritize the assets which need protection. It will also provide additional information to the group's management if the process highlights some errors in assumptions underpinning corporate strategy, especially if it leads to surprising results.

Why calculate potential liabilities?

As well as getting a better understanding of the value of core assets, companies also need to identify the costs which may arise after a cybersecurity breach so a company can decide how best to cover such an event.

In the event of any security breach, there will be a degree of additional cost. Companies will want to find out what has happened and to identify, where possible, what actions to take to prevent a similar event. This may be straightforward if the source can be easily identified, such as a result of the introduction of malware via the opening of a phishing email. However, in the case of a sophisticated attack from a third party, it may be much more difficult and time-consuming to identify the source of the breach and the extent of the damage. Where data is corrupted or deleted, there will be the cost of examining remaining data for completeness and accuracy, and the cost of restoring or re-creating the data.

Using the analysis outlined in the previous section, companies need to assess what could happen in the event of a data breach. The most commonly reported breaches are associated with the sale or publication of stolen credit card details and other personal information. Depending on the circumstances, these can be high-profile events, especially if the affected company is a household name. The reputation risk associated with such a breach will be magnified by the nature of customers' data held. The loss of credit card data can be compounded by the loss of more personal information, such as medical histories.

There are major costs associated with serious data breaches such as these, in addition to any internal management cost. These costs can include regulatory fines and a requirement to pay compensation. In some cases, affected individuals may take legal action and, if successful, may be awarded significant damages.

As with the valuation exercise, the object is to identify the potential costs associated with a breach, so that a company can decide how best to manage the risk of such events.

Return to Contents

Managing Cyberrisk

Once the company has valued its assets and identified potential liabilities at risk in the event of a breach, the final step is to manage these risks. The primary assumptions are that it is impossible to protect all assets at all times, and that all organizations will be subject to attacks at some point. These assumptions imply that some attacks will be successful. So, when setting a cyberrisk management policy, there should be three components: ensure the important data is protected; insure liabilities where appropriate; and put a response policy in place, to be activated in the event of breach.

The art of the possible

It would be a mistake simply to try to identify pressure points in the company's systems and then build a series of firewalls and other technologies to protect the system. In today's interconnected world, companies need to be able to communicate with group entities around the world: banks, suppliers and customers, as well as other third parties such as software vendors. The implementation of restrictions on communication might prevent some of the most serious attacks, but it may also act to restrict necessary communications. Too many barriers in any area will result in inefficiency and lost sales.

Any cybersecurity strategy represents a compromise between the need to have open communications with third parties, and the ability to prevent cyberbreaches. As with any corporate decision, the line between these two conflicting requirements can be drawn using a cost-benefit analysis. The exercise in the previous section should help companies develop a clearer understanding of the costs, or opportunity costs, of a security breach. The challenge in this final stage is to identify solutions to manage the risk, the costs of which reflect the potential risk to the company. As a result, companies have to decide whether to accept the risk, and then manage it, or to transfer the risk, typically by the purchase of some form of insurance.

However, it is important to reflect on the much wider definition of data at risk indicated in the earlier section to try to prioritize where any investment in protection is necessary. Realistically, all assets cannot be protected, except in very special circumstances. Companies need to ask themselves whether it really matters if a database of backed-up financial records is accessed, or whether it is more important to protect fundamental intellectual property and customers' personal and sensitive data. Most companies will need to choose to protect the assets they value the most (or the assets which if lost or made public, could give rise to the greatest level of liability).

From a treasury perspective, this means allowing innovation which improves internal efficiency via the efficient sharing of data, the centralization of decision-making and the straight-through processing of information, while recognizing that these very innovations expose companies to cyberrisk much more than ever was the case. For instance, the electronic banking communication system is no longer a standalone terminal behind a locked door. Today, electronic banking solutions are theoretically accessible from any computer with internet access – effectively not just the installed computers in the treasury group office, but also the tablet computers and cell phones used by employees during working hours and at home.

Protect the most valuable assets

Given this approach, the company should aim to prioritize any spend on protecting the most valuable assets. Given the expectation that all organizations will be subject to attack and that a breach is likely, it is usually not possible to cover every potential area of breach sufficiently, while retaining the ability to continue to do business. The cost of trying to protect all elements is likely to be both too expensive and too resource intensive, in terms of overbearing controls.

The objective therefore should be to focus time, resource and cash on protecting the most business-sensitive data.

Audit

Most companies will have some measures already in place to protect sensitive data. An audit of existing processes will identify any weaknesses and gaps. In

Return to Contents

addition, the exercises illustrated in the earlier parts of this guide may identify a number of areas where there is limited or no protection in place.

Where appropriate measures are in place, the company will also need to determine whether they are being followed consistently, whether there are any gaps in these processes, and whether any systems should be upgraded or controls tightened.

Controls

Controls should aim to limit access to specific data and systems. The risk of breach increases with the volume of individuals who have access to that information.

A key principle in managing cybersecurity is that data should only be shared on a need-to-know basis. This can be difficult to determine, but it is possible to restrict access to specific data to individuals in-house and by entity when information is shared outside the group or group headquarters. For example, a technology company manufacturing in China will only give enough information to the outsourced supplier to ensure it can fulfill the contract. This might simply be enough information to assemble the detailed component parts, without any detail regarding how to manufacture the underlying instrument. The company will not unnecessarily provide any information regarding any other element, such as the design, which represents a much more detailed risk to the company. Here the company values the IP surrounding the design much more than the IP surrounding the assembly.

Raj Bector, Oliver Wyman:

> 'Information should be shared on a need-to-know basis. Generally when information is being disseminated internally, it is appropriate to designate controls by individual. When information is being disseminated up and down the supply chain, it is appropriate to designate controls by entity.'

There also needs to be clearer definitions of when information is shared outside the organization and how this information is disseminated. Controls should be in place covering the sending of data both within and outside the organization. These controls should be relevant to the data being shared so that, for example, controls on the sharing of intellectual property or the transmission of payments will be different from those covering email. Controls must also be consistent across the organization, with some policies adopted group wide. If one staff member opens a phishing email, this can result in data corruption across the whole organization.

Scope of information security controls

ISO 27002 is an international standard describing best practice in terms of the use of controls to manage information security. The standard sets out a series of controls which good practice suggests companies should follow. These include:

- Organization of information security
  The security policy should have clear protocols for the segregation of duties, and controls for the use of mobile/portable devices and for remote working.
- Human resources security
  The security policy should start before a new employee joins an organization with, for example, references being taken up. All new and current employees should receive regular and relevant training. On cessation of employment, credentials should be canceled and other security measures, such as passwords, changed.
- Information asset management
  Wherever possible, named individuals should have responsibility for managing data assets. There should be clear policies on how data is handled.
- Access to information
  The security policy should manage access to as much information as possible. Access should be determined by business requirements: suppliers should only be given sufficient information to deliver their contracts. Within the organization, access rights and responsibilities should be given to individuals according to their role and expertise. When someone leaves, their responsibilities should not be automatically transferred to someone else. Systems should be used to manage these access rights wherever possible.

Return to Contents

- Encryption and authentication
  The security policy should set out when data should be encrypted and how information can be authenticated via the use of digital signatures and certificates.
- Physical control of systems and use of devices
  Access to systems should be controlled within buildings so that, for example, visitors are not able to enter facilities without being accompanied. There should be some physical backup of data and systems in the event of a fire or other such event.
- Operational management
  There should be a series of policies and procedures covering the operational issues. These should cover
  - training over risks from malware (these might cover how to recognize phishing emails, and whether independent storage systems such as USB pen drives can be used);
  - how and when backups should be made and how they should be stored;
  - how individual activities can be audited, including the use of log-ons/offs:
  - how faults should be dealt with;
  - who has responsibility for updating software; and
  - how administrators' rights and activities should be controlled and monitored.
- Network security and controls
  There should be a clear policy on how data should be transferred to third parties. This should include the implementation of non-disclosure agreements or contracts before any data is transferred to suppliers or other third parties.
- Responsibilities after a security event
  These should be set out clearly so that named individuals know how to respond when a security event takes place.
- Business continuity plans
  Cybersecurity should be part of a group-wide business continuity plan.
- Compliance with legal and contractual obligations
  The policy should recognize any legal and contractual obligations, and processes should be in place to ensure compliance. For example, this will include the obligation to protect any third party's intellectual property and to register with any relevant regulators.
- Audit and management reporting
  Finally, there should be a regular audit of the company's security systems.

Processes

The next stage in the protection of data is to assess whether any existing processes or procedures need to be changed. Companies will want to review the following activities:

- capture of data (e.g. credit card data);
- storage of data (e.g. latest protocols);
- communications with banks;
- communications with internal group companies, especially those in other countries; and
- communications with other third parties (e.g. software vendors, suppliers, customers).

Before making any decisions, the treasurer should help to assess the costs and benefits of making any changes.

Core treasury controls

There are a number of controls which treasurers should have in place within their departments.

- Make sure inbound and outbound data flows are free from tampering
  When adopting a new technology solution, security is an important consideration. External communications have developed very fast over recent years. All treasury management systems produce tamper-proof XML messages with the use of digital signatures and encryption.

Paul Bramwell, SVP, Treasury solutions, SunGard's corporate liquidity business:
"The real challenge for corporate treasurers is to understand the workflows built within their system and to use them as much as possible. This means knowing the formats in which files are prepared, how to ensure messages have not been tampered with and who has access to the detail within the messages."

Return to Contents

- Ensure appropriate segregation of duties
  Ultimately the key is to implement an appropriate segregation of duties, with individuals only authorized to act up to levels determined by their own competence. Most systems have multiple ways to guarantee a segregation of duties. A security map will show who has access to particular information. Systems can also tier workflow approvals, depending on the size and complexity of a deal.

  However, in small (or shrinking) departments, this can be difficult to achieve. It may be necessary to pull people in from elsewhere to support segregation such that payments or investment deals are routed through the CFO. However, this only works if the additional personnel understand the processes. It is useless and represents an additional risk if individuals asked to approve decisions are not sufficiently aware of the underlying processes. A key risk is that systems administrators also make payments because of inadequate segregation of duties.

- Reconcile activities regularly and frequently
  It is not always possible to reconcile all payments every day. However, weekly reconciliations should pick up big errors very easily.

- Manage outsourcing arrangements effectively
  Activities can be outsourced to third parties, but this works best when it is processing of relatively manual activities which is outsourced. Treasury participation is primarily when the parameters of the outsourcing agreement are set and then to manage exceptions once the system is operation.

Ultimately, treasurers need to implement the controls suggested by their banks and treasury technology suppliers. In the USA, UCC4A states that if a company follows a bank's requirements and there is a loss, then the bank has to take responsibility. In Europe, the Payment Services Directive contains similar conditions, although it is less beneficial for companies.

Brian Welch, Director at the UserCare Treasury Consultancy:
"There are three keys to managing cyberrisk when processing payments. First, implement the security controls suggested by your banks and technology vendors. Second, regulations including the US UCC4A and the Payment Services Directive provide a degree of protection should things go wrong. Third, identify as quickly as possible if a payment goes astray. A missing large payment will be identified quickly. Smaller ones should be picked up in the reconciliation process."

Using mobile technology to manage treasury activities

There is increasing interest in mobile technology to manage treasury activities. Some applications are fine but they are, by design, limited. As with other activities, the protocols for the use of mobile technology within the organization and within the department need to be clearly established.

There are a number of key questions which need to be addressed:

- What happens if supporting data or documentation is required to make a decision? It may be appropriate to acknowledge receipt of request for the approval of a transaction and then return to office to determine the approval.
- Are mobile technologies secure? It is vital that devices cannot be compromised if they are to be used to communicate key decisions. For example, it may be appropriate to use a mobile device if the treasurer is onsite but in meetings and connected to the virtual private network. The use of public wi-fi is much less secure.
- What happens if people lose their phone? What data is held on the machine? Are credentials held on the machine?

Return to Contents

Review

As part of the ongoing cyberrisk management strategy, the company should regularly review all processes for effectiveness and make sure they are audited for compliance.

There should be a committee or group responsible to the board for the management of cyberrisk. It needs to be tasked with continuous improvement, as the nature and extent of cyberrisk changes with time.

Manage the remainder

The purchase of cyberinsurance has increased over recent years. Insurers have seen significant increases in the number of companies reviewing cyberinsurance, the number of new buyers of cyberinsurance and an increase in the volume of coverage being purchased by both.

Before purchasing any insurance, the treasurer should help the company understand what insurance is already in place, and carry out coverage gap analysis. If the company does not have an enterprise-wide risk management committee, the cybersecurity committee needs to identify who else manages risk. The key is to communicate effectively across departments.

With knowledge of where coverage gaps are, companies can then identify where they might want to purchase insurance. As with other insurance, the purchase of cyberinsurance is essentially a cost-benefit decision. The valuations described in the previous section can be used to determine whether the cost of premiums is appropriate for the value of assets and cost of liabilities being protected.

How can insurance help?

Insurance can provide protection against a number of cyber-related events, both first-party costs (those incurred by the affected party directly) and third-party costs (liabilities arising from the impact on customers and suppliers of the affected party).

In terms of first-party costs, insurance can provide cover for the cost of re-creating data and restoring systems to a serviceable state. It can also cover the cost of responding to a cyber event. These costs can include the cost of identifying the source and extent of the breach, the cost of notifying the appropriate authorities and third parties, and costs associated with public relations and communications management. This may include the cost of appointing legal representation to communicate with regulators, or advisors to help navigate regulatory compliance. For example, there are US federal and state laws requiring certain actions in the event of a breach. In California, the breach notification statute requires an affected company to inform people of a data breach and to make an offer of compensation. Finally, some policies may also provide cover for a loss of income and increased operating expenses in the event of a technology failure.

In terms of third-party costs, insurance can cover a wide range of liabilities. Typically, liability coverage is limited to providing a defense to any alleged claims of harm, and indemnification for damages or loss for which the policyholder is legally liable. Cyberinsurance provides typical liability coverage, but cover needs to go beyond this, to capture expenses that are not directly tied to a claim or are incurred prior to the allegation of a claim. Such expenses can include privacy liability (which can be significant in the case of data which identifies individuals) and the costs of any regulatory fines and victim compensation, any data breach arising as a result of the affected party's data breach (e.g. compromise of a supply chain database which includes supplier details as a result of a virus affecting network security), and other liabilities. Where a breach occurs at an outsourced partner (e.g. data is lost by a Cloud vendor), the policy will respond as if the breach had taken place at the policy-holder's premises.

Robert Parisi, FINPRO Cyber & Technology Product Lead, Marsh:

"You can manage risks in a number of ways: by policy and procedures, through the use of technology and by purchasing insurance. Insurance is for that residual risk where additional policy or procedures would not prevent or mitigate the risks."

How is cyberrisk insurance underwritten?

Although there has been a significant increase in underwriting scrutiny of cyber policies over recent

Return to Contents

years, the model remains fairly rudimentary, with only a relatively small number of counterparties.

Before entering into an insurance contract, the underwriters will want to make an assessment of the company's cyberrisk management policies and procedures. The underwriters will spend some time assessing the controls in place at the company. The assessment focuses on the cybersecurity from a governance or policy and procedure perspective, rather than an investigation or verification of implementation. The company will be required to maintain a similar or equivalent level of these controls, taking into consideration the changing and evolving threat environment. At this stage, most companies have appropriate controls; few are outstanding across all areas, and few are weak across the board.

In particularly, underwriters and regulators will want controls to cover the encryption of data, especially sensitive financial data in flight, data on mobile and portable devices, and on backup systems. Policies should be clearly defined, with individuals clearly responsible for specific actions. These policies should be supported by regular training of both current and new employees.

Underwriters may help with the quantification process described in the previous section, and will be able to explain some of the potential liabilities in the event of loss. From the company's perspective, the purpose should be to try to understand what coverage is in place already, if any, how much additional coverage is required, and whether the premium is aligned with the risk. Although coverage applies globally, the location where most business is done (and therefore whose data is held and what regulations are most likely to come into play in the event of a breach) will make a significant difference in the level of the premium.

Policy in the event of breach

The final element of any cybersecurity policy is to determine how to react in the event of breach. It is likely that a company will be subject to some form of attack at some point during the year. The measures in place above should help to minimize the risk that any attacks will result in breach. However, it is possible that a breach will occur, so prudent planning requires a policy and set of procedures to be in place.

Crisis response plan

As discussed, it remains likely that all companies will experience a cybersecurity breach at some point in the future, although the costs to affected companies will vary significantly.

The purpose of a crisis response plan is to minimize the impact of a breach, in both the short and long term. Despite this, many companies have yet to adopt even a basic crisis response plan. The *2015 AFP Risk Survey* found that 60% of companies do 'not have a clear, documented mechanism to respond to a cyberbreach event'. Although the development of a plan will be specific to each organization, frameworks are available from a number of institutions, including the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO, see page 12). These could be used as a basis for a new plan. Each crisis response plan should include the following elements:

- Adopt a crisis plan

  Having even a rudimentary crisis response plan will help the company adopt a more coordinated approach. Where companies have crisis response plans, they are often integrated into their disaster recovery and business continuity plans.

- Manage communications

  Once a cybersecurity breach has been discovered, the company needs to manage its communications, both internally and externally (including with law enforcement agencies and regulators). The crisis response plan should state individual responsibilities for managing communications and determine what information is shared. It should also set out, step by step, who should be called, and when. It should state clearly which organization should be called first: this could be law enforcement or another government authority.

- Analyze the breach
  - How was the event uncovered?
  - Who and what caused the breach?
  - How long has it been operational?

Return to Contents

  - How has data been affected? Has data been corrupted, stolen or lost? If so, whose data has been affected?
  - How does the data breach affect the ongoing operations of the business? Can business operations continue as normal?

- Manage the immediate consequences

  Relationships with affected customers, suppliers and other parties need to be managed.

  Regulatory requirements must be met. This may involve the payment of compensation.

  The company may also need to manage public relations, if the breach is high-profile.

- Improve

  The company must have a process which allows it to learn from its mistakes. This may involve implementing additional training.

- Review

  Finally, the company should regularly review and test its crisis response plan.

The crisis response strategy needs to sit within a broader business continuity plan. This will deal with the longer-term consequences: law suits, fines, reputational impact and loss of income. It is important to understand the role of business continuity plans. Enterprise risk management requires the company to understand its risk appetite and to take appropriate action to either accept or transfer the risk, or to change behavior. Business continuity plans should be designed to help the company plan for, and respond to, incidents and business disruptions, so that the company can continue to operate at a predetermined level. Within this level of planning, disaster recovery plans help companies recover immediately and have access to critical infrastructure in the short-term. Insurance may compensate for some of the costs associated with such events, but it cannot ensure operational continuity.

Martin Eggleton, Director, Moas Consulting Ltd:

"The key to a successful business continuity plan is to overcome complacency. This means understanding the gaps between what the management thinks they have, what the company actually has and what they need."

Return to Contents

Conclusion

As the question of how best to manage cybersecurity advances up the corporate agenda, treasurers can play a valuable role in helping to prioritize their company's responses.

This guide has outlined a three-stage approach to implementing a cybersecurity management policy. The first step is to work to understand the nature of the data which is at risk. This requires companies to understand where cyberthreats are most likely to come from: fraud and error perpetrated by current employees remain the most common source of threat. Companies also need to understand fully the scope of data and information they hold, and how any compromise of security may lead to financial loss.

Once the company has a clear view of the data it holds, the next step is to value this data and assess the potential liabilities in the event of loss.

With an understanding of the most valuable pieces of data, the final stage is to establish a security management policy. This should involve putting in place systems and controls to protect the most valuable assets and using insurance to protect the company against the consequences of data loss or corruption. Finally, companies should expect data breaches from time to time. Companies should have a crisis response plan to help minimize the impact of any data breaches.

Return to Contents

Checklist for Identifying Assets

All organizations hold a range of data. This checklist is designed to help the cybersecurity management team identify the full range of assets to be valued and how any loss or corruption of that data could affect the organization. Note that the precise nature of assets will vary by industry and business, and certain assets will be more important in some industries than others.

Internal assets

- Human resources records

  Companies have to hold a significant amount of highly sensitive human resources records. This can include personal information, including health records and performance information. Loss of human resources can result in significant embarrassment for the company and the requirement to pay restorative damages.

- Customer data

  All companies hold a degree of customer data, the nature of which is determined by the type of industry in which the company operates. Companies in the retail industry are more likely to hold individuals' credit card and other personal data (such as addresses). Some companies may hold more personal data, such as medical records, on behalf of their customers. Others may hold their customers' intellectual property, if they produce product on a subcontracted basis. Others may hold data of a classified nature, if they are a supplier to a government, for example. In each case, there are potentially serious consequences in the event of a security breach, not least to the company's reputation and, therefore, its ability to do repeat business.

- Intellectual property

  One of a company's core data sets is its intellectual property. This varies according to the nature of the company's activities, but is likely to include formulae, blueprints, production processes and techniques, and methodologies. The very real risk here is that any acquisition of this data by competitors will allow them to erode any competitive advantage the company might have, threatening the long-term future of the business. In some industries, the loss of IP can also result in additional security problems, whether a hardware basis (such as in the military goods industry) or a software basis, where the lost IP is in the form of code.

- Negotiating positions

  If a company's negotiating positions before or during a tender or renewal process are disclosed, other parties can benefit to the detriment of the company. Third parties may be able to undercut a tender price. A company awarding a contract may be able to negotiate down to the other company's red lines, reducing its profitability.

- Strategy documents

  The leak of strategy documents can help third parties to counter and even anticipate key future developments by the company. For example, a third party may bring a product launch forward to disrupt marketing plans, it may purchase real estate or open a new outlet in an area it becomes aware is of interest to the other company, or it may enter into negotiations with target acquisitions to disrupt future expansion of the third party.

- Internal email and other messages

  Much of the above information needs to be shared by different parties within the organization. For example, much of the group's intellectual property will need to be shared between research and development and the group's various production facilities. Negotiating positions will be shared with the negotiating team as well as senior figures within the organization. The transmission of this information between interested parties is a separate cyberrisk, as there is the risk of information being shared outside the approved group or of messages being lost or corrupted. One of the big challenges is to ensure messages are noted, understood and, where necessary, acted upon by the required recipients. Delays in the receipt of messages (perhaps when a key player is out of the office visiting group locations around the world) can result in problems.

Return to Contents

Treasury-specific assets

- **Financial positions**

  Companies hold a lot of sensitive financial positions, including payment records, bank account information and tax information. Companies rely on this information to manage their businesses efficiently and to ensure cash is available to business units to fund activities, including expansion. The loss or corruption of this data can make decision-making more difficult until the data can be restored in a verifiably accurate way. Second, some financial information can be embarrassing when made public. For example, recent allegations of multinational corporations taking advantage of tax-efficient structures to minimize their liability to corporation tax have been well publicized and have caused some reputational damage to the companies concerned. Although the amount of tax paid is a matter of public record, the calculations and filings on which they are based is not.

- **Payment initiations and approvals**

  All companies must have processes to initiate and approve payment instructions. The use of technology and the centralization of decision-making together mean that increasingly these activities are performed electronically. This requires communications, often via the internet, and may include remote access for individuals to approve payments. The risk is that these protocols are breached, allowing payments to be approved by non-authorized individuals or to be changed before the instructions are submitted to the bank. In addition, there is a risk that reconciliations may also be affected through a similar breach, the primary risk being that a fraudulent transaction is falsely reconciled and therefore not identified during regular audit activity.

- **In-house treasury structures**

  Any in-house treasury structures rely on the communication of data between group entities. In most cases, the structures are operated by banks which hold bank accounts in the name of different group entities. However, it is possible for companies to operate in-house banking structures where the group treasury holds a bank account for the group as a whole, making disbursements and collecting payments on behalf of all group entities. In this scenario, group entities communicate with the group treasury directly, submitting transaction information for the treasury (or payment and collection factory) to process on their behalf. Any disruption to this communication can have significant consequences for the group as a whole.

External

Companies also have to be aware of the risk to data held outside or sent outside the company. The primary risks include:

- **Intellectual property**

  Some companies will need to hold intellectual property owned by the company. For example, where activities are outsourced to a supplier, there must be a degree of information-sharing along the supply chain. Understanding the limit of what needs to be shared helps to reduce exposure to cyberrisk in an outsourced contract.

- **Outsourced processes**

  Other outsourced processes can also be subject to cyberrisk. Ideally, activities will be outsourced on a service-level basis, such that the outsourcing partner will be able to operate within pre-agreed parameters.

- **Data stored remotely and in the Cloud**

  After some high-profile examples of data stored in the Cloud being stolen or illegally accessed, companies will be concerned over the security of their data held outside their firewalls. Areas to be concerned include any remote backup of corporate systems. It is prudent to have a remote backup for business continuity purposes. However, the company will want to ensure that the location of the stored data is secure and that the method of transmitting data to this location is similarly secure.

- **Payments**

  Companies are also sensitive about the security of payment instructions to both banks and suppliers. This will range from ensuring the authenticity of payment instructions, encrypting data in flight, and

Return to Contents

ensuring that settlement instructions are accurate and have not been compromised. Because of the speed of payment message transmission and the use of encryption, the risk of payment interception is less likely to cause loss than payment fraud. Companies should have appropriate reconciliation processes in place as an additional check.

- **Misdirected communications**
  One of the easiest mistakes to make when sending email and other messages is to misdirect them, either by the use of inaccurate addresses or by copying in third parties. This can result in the loss of intellectual property, and other events illustrated above. Forwarding email messages can also result in data being inadvertently submitted to third parties. There are additional risks associated with the use of smartphones which can anticipate recipients, for example, and allow messages to be sent with minimal user involvement.

- **Supply chain**
  Finally, in today's environment, there is a much greater degree of information-sharing along supply chains. From a sales perspective, it makes sense to share information with a view to reducing uncertainty and therefore cost along the supply chain, allowing greater flexibility when setting the final price and providing for greater scope to compete in the market place. From a financing perspective, it makes sense for creditworthy companies to use their access to credit to finance suppliers and, in some cases, customers. All these developments mean it is important to share information along the supply chain. Companies need to ensure they only allow suppliers and customers access to the information they need to know. For financing solutions, companies need to be able to restrict access to ensure only individuals authorized to access platforms are able to do so, and that data entered can be authenticated.

Return to Contents

About the Author

WWCP LIMITED

WWCP's team of financial researchers, journalists and authors provides its WorldWideCountryProfiles service to banks, financial institutions and professional bodies. Purchasers use the individual country profiles, which are researched and written to their specification, for their customers and prospects, sales literature, their intranet and extranet sites and sales training. WWCP researches over 190 countries.

WWCP researches, authors and publishes authoritative Treasury Managers' Handbooks for: Africa; the Americas (five editions); Asia/Pacific & Australasia; Central & Eastern Europe; Europe (five editions); Middle East and Scandinavia/Nordic/Baltic countries.

Publications also include a number of definitive WWCP authored treasury guides: Best Practice and Terminology; with The ACT, Investing Cash Globally (four editions), International Cash Management and Trade Finance; and, with AFP, Treasury Technology and a series of treasury guides.

www.worldwidecountryprofiles.com www.wwcp.net

Return to Contents

Corporate Treasurers Council

The Corporate Treasurers Council is the executive-level membership of AFP. The CTC features tailor-made products, events and exclusive networking opportunities all year long for treasury and finance executives that address the latest industry insights, trends and best practices and will provide guidance, practical tools and the validation needed to move forward in making critical decisions.

When you join AFP and have the title of *corporate treasurer, assistant treasurer, chief financial officer, vice president of finance or controller*, you are automatically enrolled in the Corporate Treasurers Council (CTC) and have access to CTC products and events.

For more information go to www.corporatetreasurers.org

ASSOCIATION FOR FINANCIAL PROFESSIONALS

About the Association for Financial Professionals

Headquartered outside Washington, D.C., the Association for Financial Professionals (AFP) is the professional society that represents finance executives globally. AFP established and administers the Certified Treasury Professional™ and Certified Corporate FP&A Professional™ credentials, which set standards of excellence in finance. The quarterly AFP Corporate Cash Indicators™ serve as a bellwether of economic growth. The AFP Annual Conference is the largest networking event for corporate finance professionals in the world.

General Inquiries	AFP@AFPonline.org
Web Site	www.AFPonline.org
Phone	+1 301.907.2862

Return to Contents