# Cybercrime – Stealing in the Connected Age
# Survey Results

Treasury Alliance Group LLC
www.treasuryalliance.com

February 2016

# Executive Summary

- Cybercrime is a growing problem in the world of treasury. As part of a recent seminar on cybercrime, TAG asked a group of 188 treasury professionals a series of questions related to their experience of cybercrime and what their companies were doing to help protect themselves and their customers. Cybercriminals are everywhere. And, although they are after all forms of sensitive data, treasury professionals are often more directly effected as many cybercrimes are financial in nature.

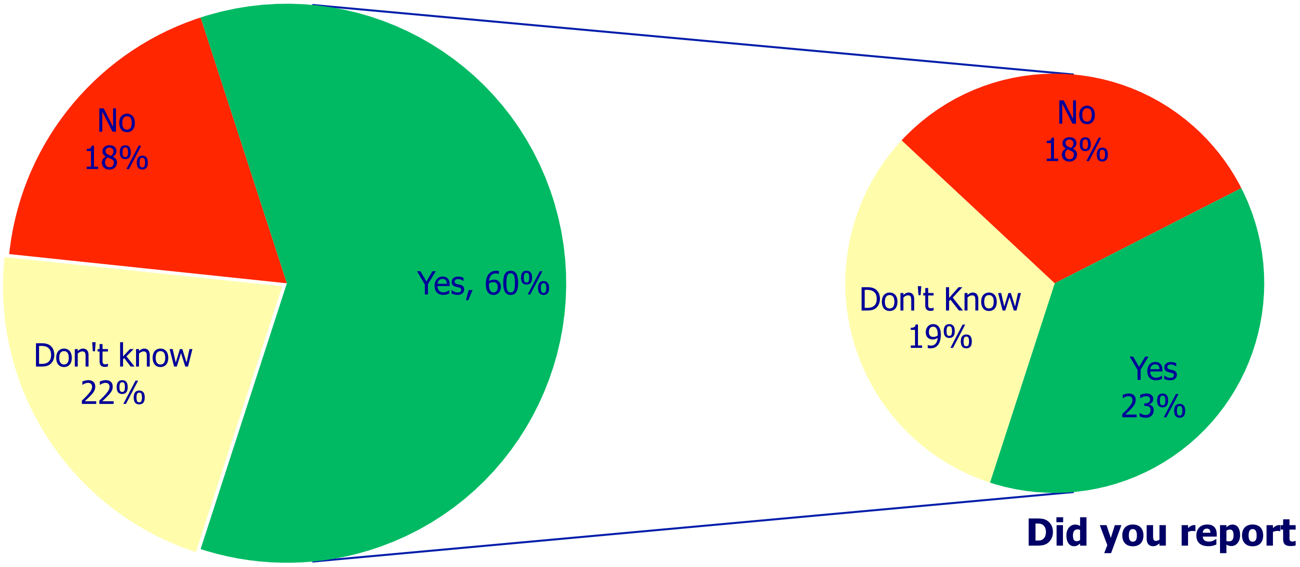
- Key findings of this report include:
  - 60% of all respondents have been the targets of cybercrime
  - Mobile access to company data and email is becoming ubiquitous
  - Most companies are taking basic measures around passwords to protect themselves
  - Many companies have implemented formal cybercrime policies
  - A growing number of companies are purchasing cyber liability insurance

- Based on our survey results, cybercrime is an area of concern for most treasury professionals. This report will provide  detailed results that were identified by the survey. During the webinar TAG provided a number of best practices and pragmatic recommendations that companies can implement to help protect themselves and reduce their exposure. An excellent first step, however, is to conduct a security review to identify and quantify potential risks or problems and document the controls already have in place. More information, including a recording of the full webinar is available on the TAG website.

# Figures

# Cybercrime – A Growing Threat

60% of survey participants indicated that they had been the target of cybercrime. This supports the 2015 AFP Payments Fraud Report in which 62% of survey respondents indicated that they had been targeted in the prior year.



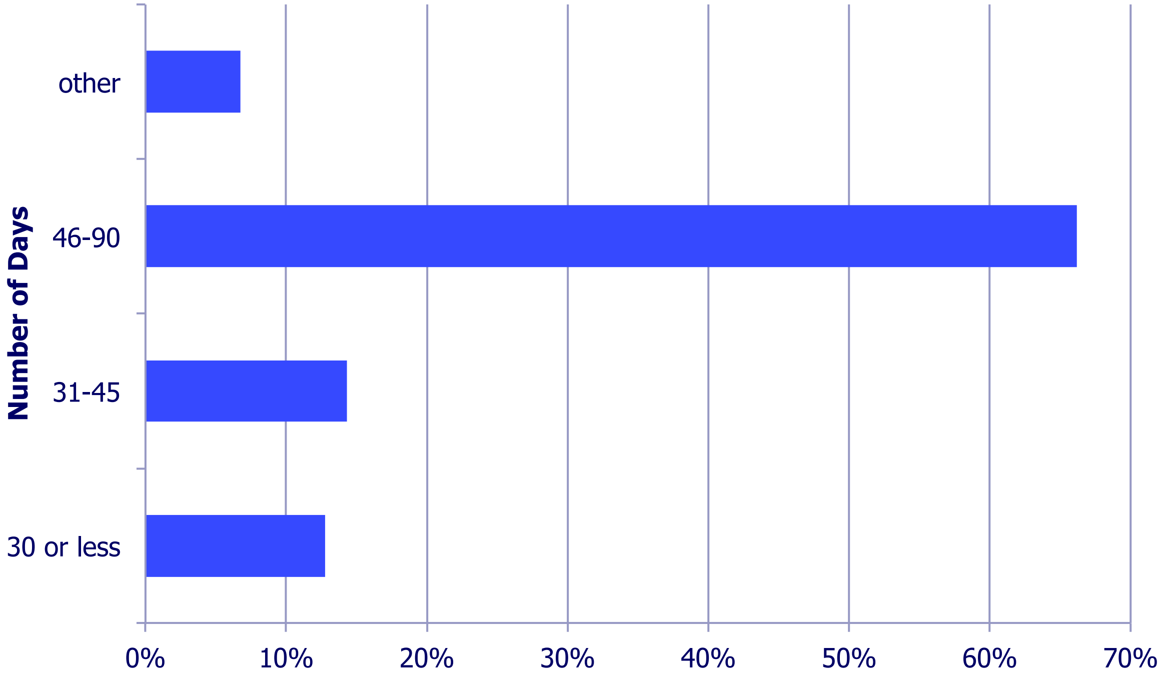
**Did you report it?**

Somewhat more surprising was the fact that just over 1/3 of those who had been targeted (23% of the respondents) said they had reported the attempt to the authorities. TAG believes that reporting cybercrime is a best practice and is often required by insurance carriers if a claim is filed.

# Password Changes

Passwords are the initial control of most online and internet systems. The use of strong passwords coupled with periodic changes of those passwords is a best practice in the industry. 96% of respondents indicated that their companies required them to periodically change their passwords. 66% of the respondents are required to change their passwords every 46-90 days with 13% changing them every 30 days.

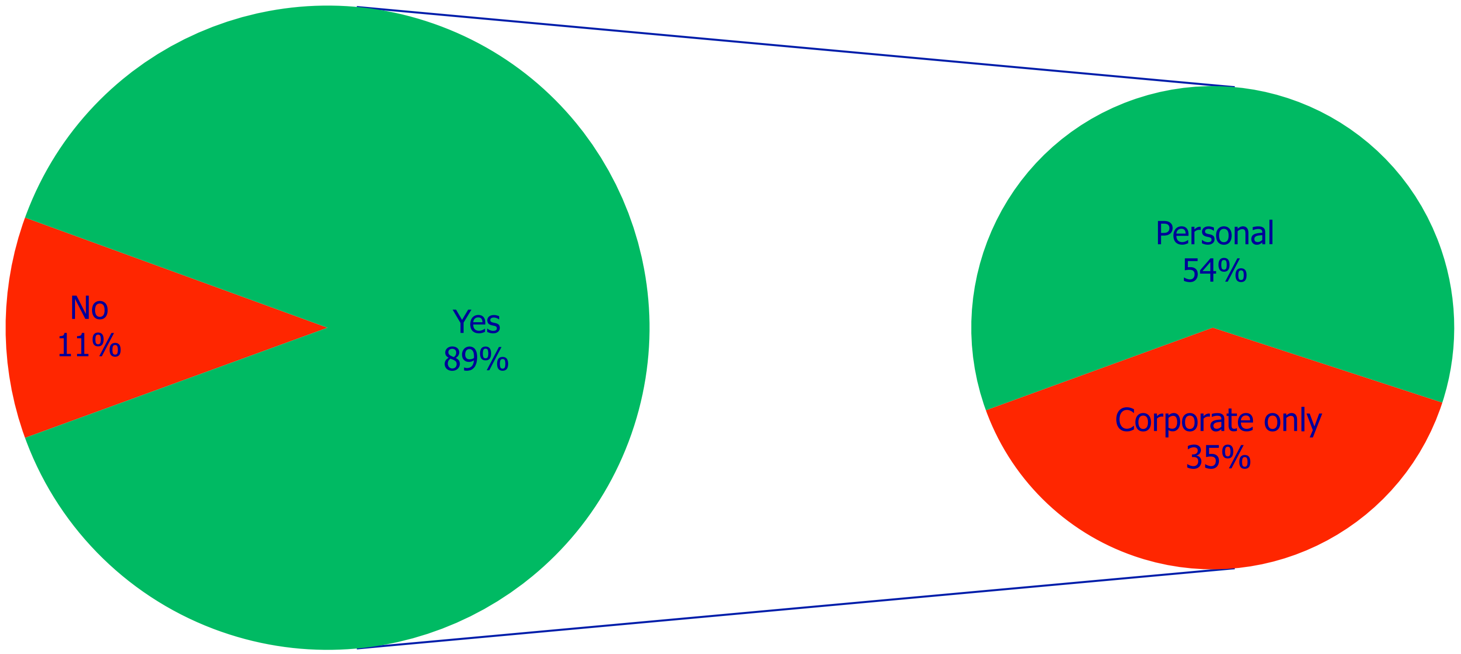
## Frequency of Password Change



# Mobile Access

Mobile access to company data and email is an area of risk that concerns many companies. Until fairly recently, most companies either did not allow mobile access or limited it to company provided devices such as Blackberries. This has changed as employees have become used to mobile access to data in their personal lives and are now demanding it in their corporate lives. 89% of the respondents now have remote access to company data with the majority of them, 54% allowed to use their personal mobile devices.

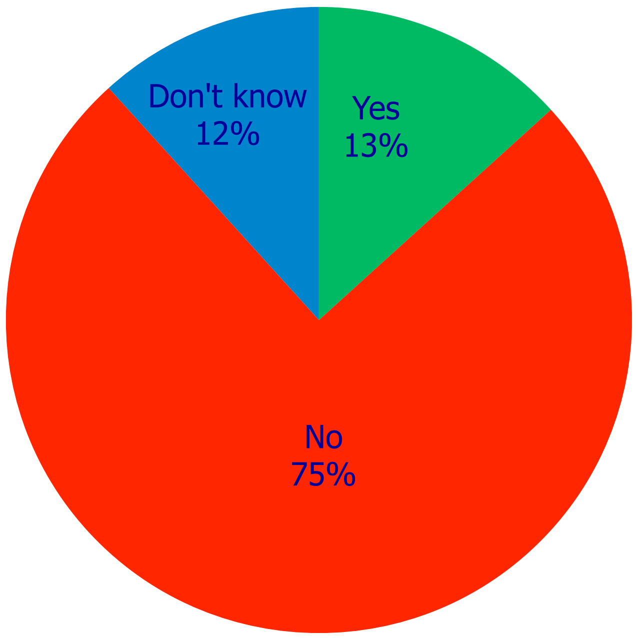
## Use of mobile devices to access company data and email



# Limited Use Payments Workstations

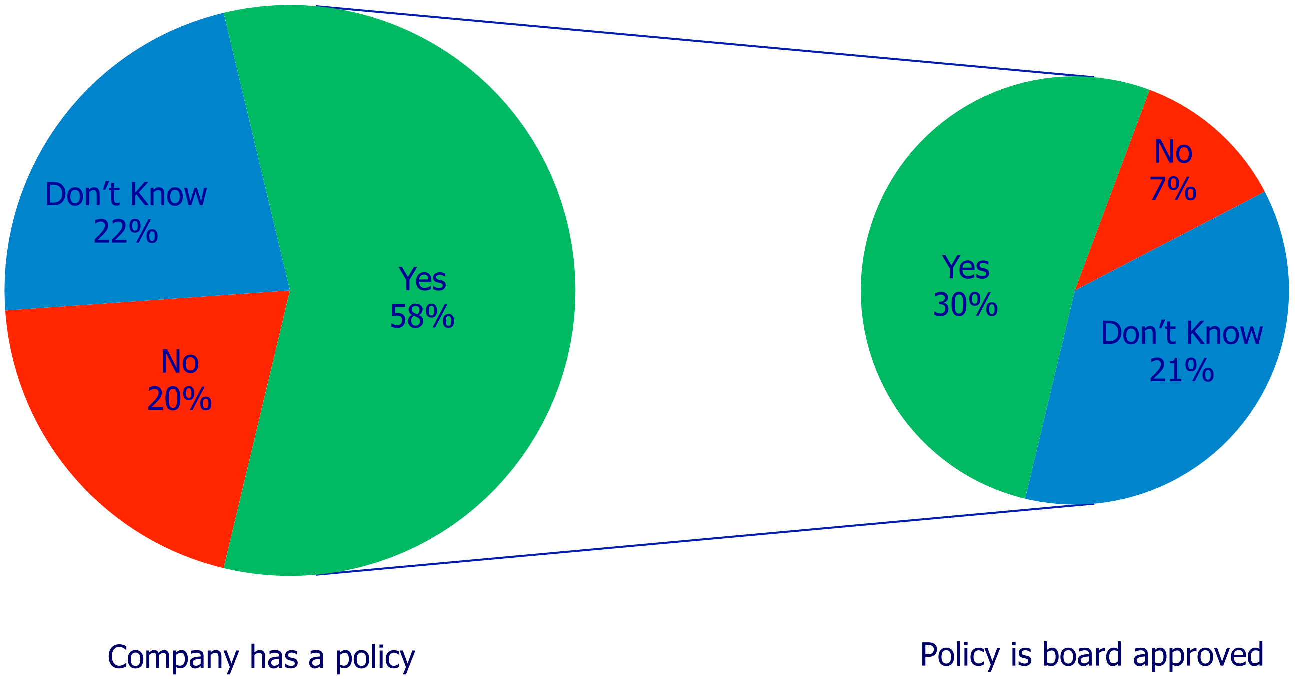
TAG has long recommended the use of a dedicated workstation or terminal with limited internet access for online payments. The combination of low cost computers/work stations and browser based payment software has made this an easy and fairly cost effective safety measure. Given the prevalence of online malware and account takeover attempts it was a surprise that very few of the respondents report using a dedicated terminal for payments initiation.

## Does your company use a limited use workstation for payments initiation?



# Cybercrime Policy

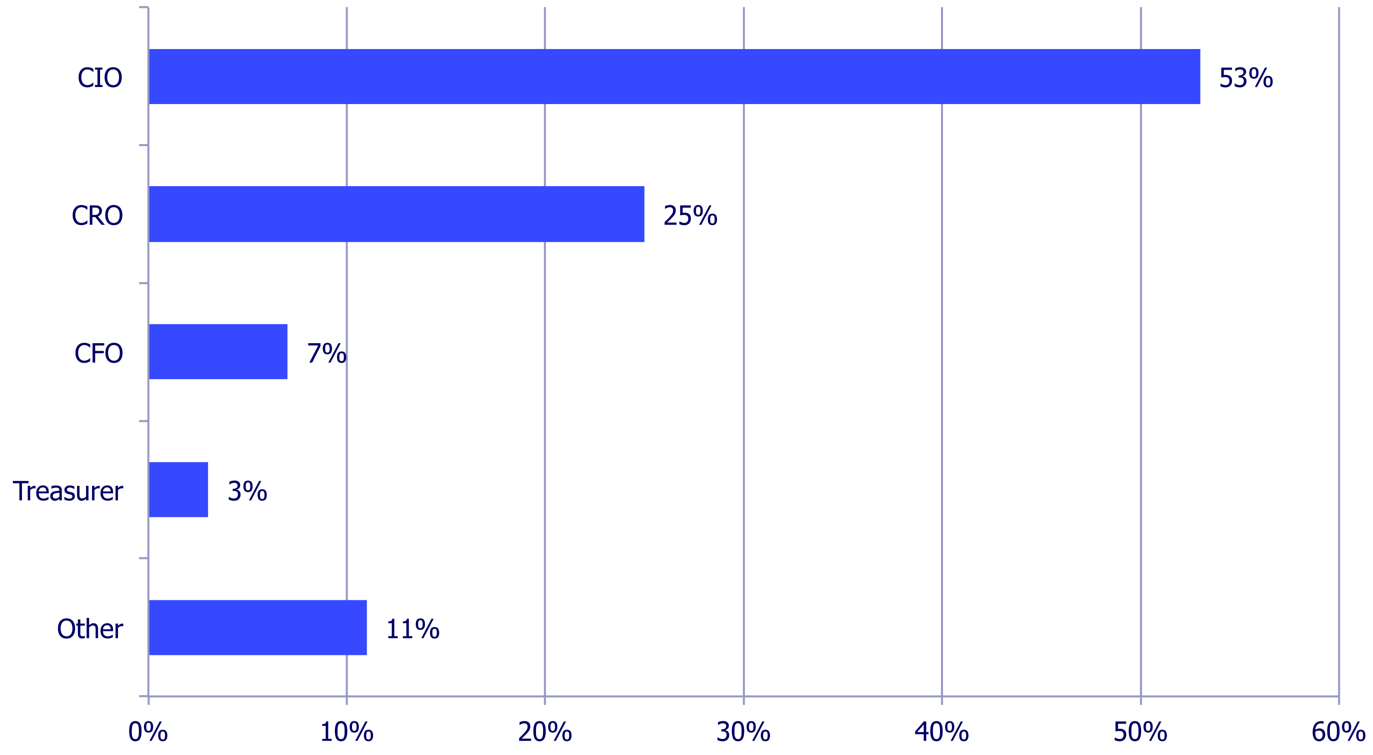
The growth in both internet business and cybercrime itself has increased the need for formal cybercrime policies that discuss how a company will protect itself –and its personal and customer data - and what it will do if attacked. As with other corporate policies, board approval and oversight are a best practice. Just over half, 58% of the respondents indicated that they did have a formal policy, and  just over half of those policies were board approved.



# Policy Responsibility

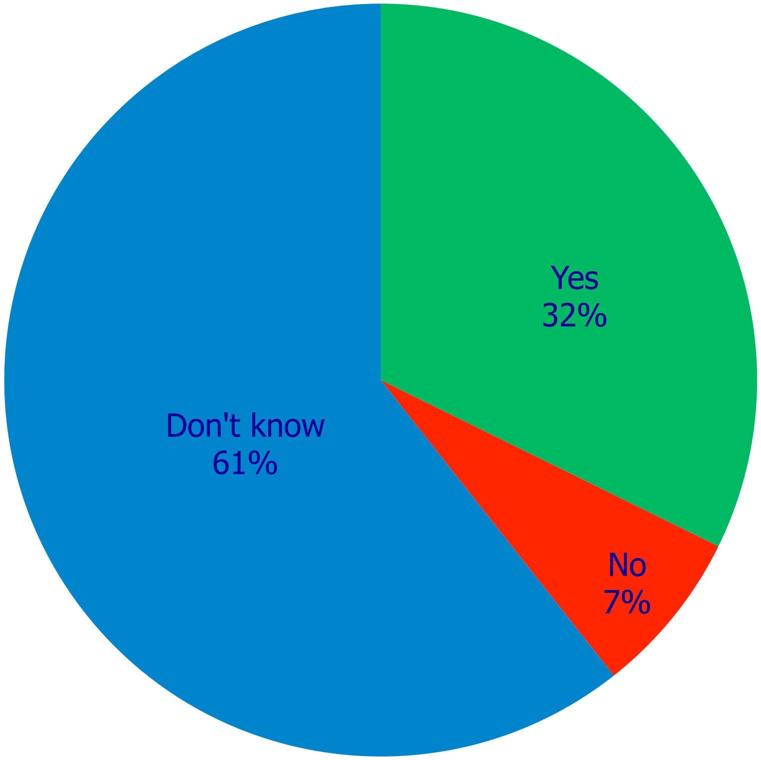
The Chief Information Officer or head of IT was the corporate officer usually responsible with managing the cybercrime policy. Presumably because of the potential financial impact of cybercrime, there were a number of respondents who had given this responsibility to their CFO or Treasurer.

## Responsible for Cybercrime Policy



# Use of Cyber Liability Insurance

Cyber liability insurance is a growing product in the insurance industry. Although specialty insurers have provided computer insurance for many years, cyber liability policies are relatively new and can cover both direct and indirect costs related to cybercrime. Many companies assume these costs are covered by standard liability policies. But increasingly cyber risks are being excluded from basic liability coverage as insurers turn to specialized policies. Just under 1/3 of the respondents indicated that their companies currently have some form of cyber liability coverage.



# About Treasury Alliance Group

Since 1981, Treasury Alliance Group and its predecessor firms have provided treasury and payments consulting services to over 400 clients in 42 countries. As a result, we have broad knowledge of best practices from working with “world-class” organizations in a wide variety of engagements. Our experience insures practical, realistic solutions that meet our client's unique requirements.

Our Partners are all experienced senior-level treasury professionals with experience in all facets of treasury management, payments and bank operations, as well as operating experience in both the corporate and banking arenas. Our partners are acknowledged leaders in the industry who frequently teach, write, and present on a variety of treasury management and payment topics.

We have worked with clients in a wide variety of industries in both the private and public sector. They range in size from large Fortune 100 companies, government institutions multinational banks to small privately-held concerns.

Please visit our website at www.treasuryalliance.com for further details and articles and presentations on key topics in global treasury and payments.

# Contact Information

Daniel L. Blumen, CTP, Partner
Phone (630) 717-9728
dlblumen@treasuryalliance.com

Mark K. Webster, CCM, CPA, Partner
Phone (216) 932-1678
mark.webster@treasuryalliance.com

Treasury Alliance Group LLC
www.treasuryalliance.com