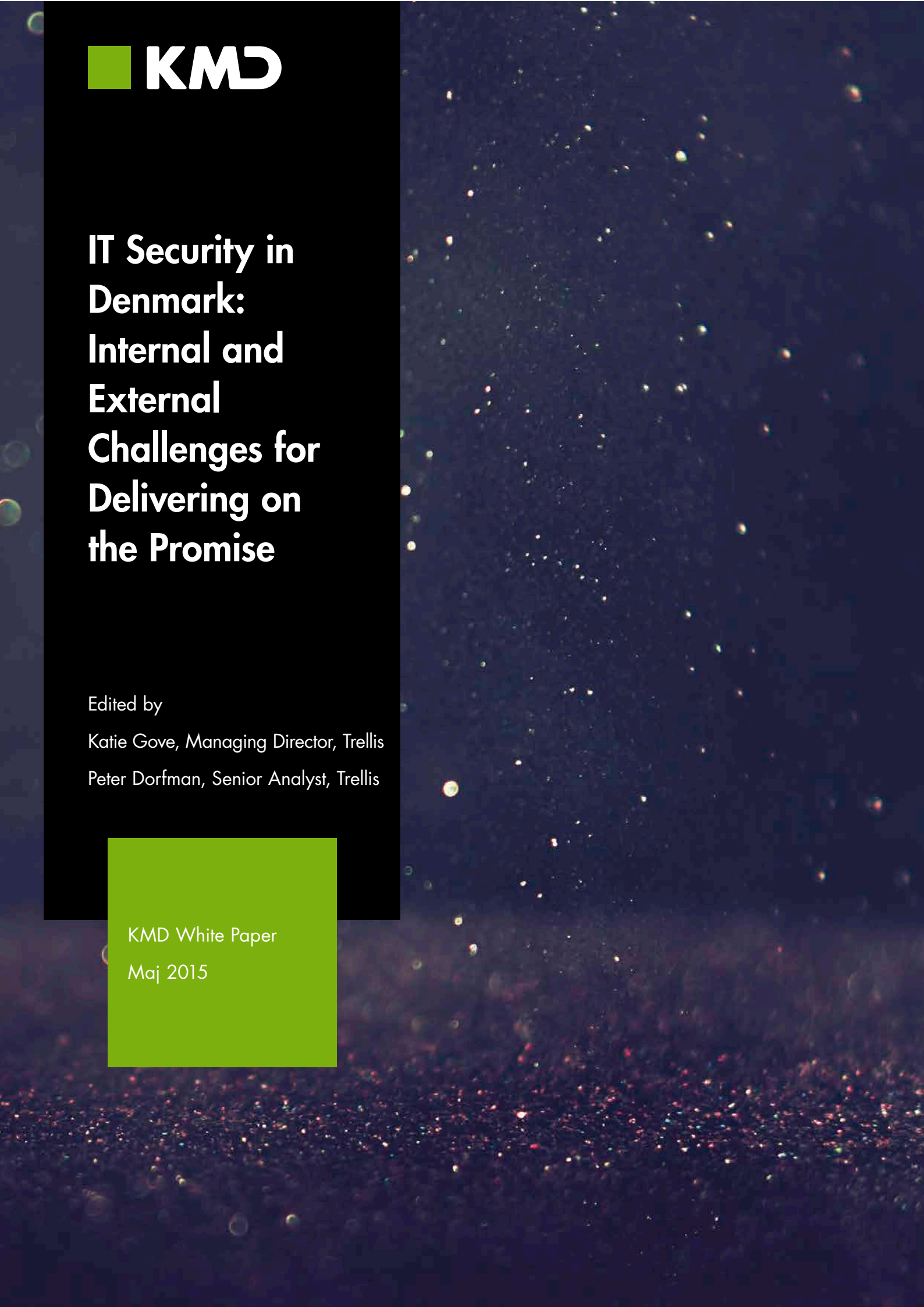

IT Security in Denmark: Internal and External Challenges for Delivering on the Promise

Edited by

Katie Gove, Managing Director, Trellis

Peter Dorfman, Senior Analyst, Trellis

KMD White Paper

Maj 2015

Table of Contents:

Maj 2015

I am in daily contact with talented technical and strategic IT professionals primarily working in the Nordic countries but also working in other markets in Europe, not to mention key markets in North America and Asia. I am often impressed and inspired by the professionalism and technical competencies that I see across the board.

One common thread across many markets is that the speed of change, that is, the move to almost complete digitalization of both work process and assets, is something that has often out-paced the ability of security functions to keep pace. Coupled with the extreme pace of change is the dark reality of the financial crisis that has profoundly limited organizations', both public and private, abilities to invest appropriately not only for growth but also for security.

In Denmark, our governments have until recently been reluctant to sign a national IT security strategy which in other countries has been instrumental in helping companies and public sector bodies to be able to develop security policies and to establish a business case for investing in IT security.

The results of KMD's latest round of research into IT security in our market help to illustrate the reality of IT security. The picture that is drawn is one of a market focused primarily on technical compliance to established regulations.

The study characterizes the "default setting" for IT security of the majority of Danish organizations as being events-based and reactive rather than proactive and strategic. Fundamental reasons as pointed out by more than a few study participants relate to the overly operationally-focused organizational structure of IT organizations and the challenge of truly manifesting strategic business goals via visionary leveraging of IT.

Worryingly, several of the CISOs and CIOs contributing to the study pointedly note that their organizations feel overwhelmed in ascertaining where they should invest limited time and resources in facing such an enormous challenge.

The silver lining in the research is the growing attention and activity around identity management (roles and responsibility), event logging, and behavior. Centered around the user and made truly possible when supported by consistent training, this growing focus on human activity and interaction is necessary as well as appropriate and has long been a part of KMD's internal practices and client services.

I am quite sure that the conclusions presented in this research will provide a solid basis for discussion for our market to come to grips with not only the external challenges but also the insider challenges presented by IT security in our modern digital world. I look forward to being part of this dialog with our clients, partners and markets.

Rasmus Kærsgaard Theede
VP, Group Quality & Security, KMD

INTRODUCTION

In September 2014, KMD released its white paper "IT Security: It's Everybody's Business," the result of a survey of 31 CIOs from some of Denmark's largest firms, probing the status of security practices and investment. That study found that Danish firms appear to be lagging companies in larger markets, not just in terms of investment in security tools, processes and staff, but seemingly in awareness of and concern for effective data protection practices.

This new white paper presents the results of a follow-up survey digging deeper into specific attitudes about the threat of data security breaches, the ways in which companies invest in security and the drivers for increasing support for that investment.

Methodology

This survey is based on quantitative and qualitative data input from 34 CIOs and CISOs at some of Denmark's 300 largest private enterprises. Respondents were assured that their data would be kept anonymous. More than a few also agreed to follow-up interviews – their comments are presented herein, attributed to them only as individuals from specific industries.

The data once again depict a business culture in Denmark that is relatively passive in its attitudes toward data security, although respondents project modest increases in security investment in the coming year. They suggest that modest growth in executive support for security measures is due largely to new regulations expected in 2015 and to increasing media coverage of high-profile data breaches. But the study's CIOs and CISOs tend to feel their companies are more concerned about the fallout from compliance issues created by new Danish and EU regulations – sanctions, fines and negative publicity – than about the actual damage that might result from a breach of their own systems.

A key takeaway from this new survey is that Danish executives continue to regard spending on IT security as a cost – as overhead – rather than an investment in quality.

Danish executives are waiting for a "smoking gun" to prompt greater investment in IT Security.

Some of the survey's questions provided the opportunity to respond (e.g., Agree or Disagree) or to respond emphatically (Completely Agree or Disagree). Respondents are somewhat guarded in their answers to these questions – they have clear but rarely emphatic opinions about security issues, suggesting that these executives may have reservations or an intuition that trends related to IT security may change in the foreseeable future.

Asked what it will take to change executive attitudes toward security, the study's participants offered diverse ideas, but the most popular response was that it is likely to require a large Danish enterprise to suffer a significant, highly publicized breach – a "smoking gun" that would provide an object lesson and demand reaction.

Yet one CIO observed ironically, "We do read the international news. We've heard about Sony and Target. And we have had some notable cases in our market. Maybe heads haven't rolled here but, it's been big stuff. I think that we read about these cases and think that somehow we're different or better or

exempt." He went on to say, "Maybe each company has to experience its own crisis for us to change."

LEVEL OF CONCERN

A striking finding of the survey is the generally low level of vigilance among Danish companies toward data security. Respondents were asked to evaluate their companies' overall approach to security, characterizing it as "Proactive and strategic" or "Events-focused" (meaning passive or reactive). A slight majority characterized their companies as reactive toward security.

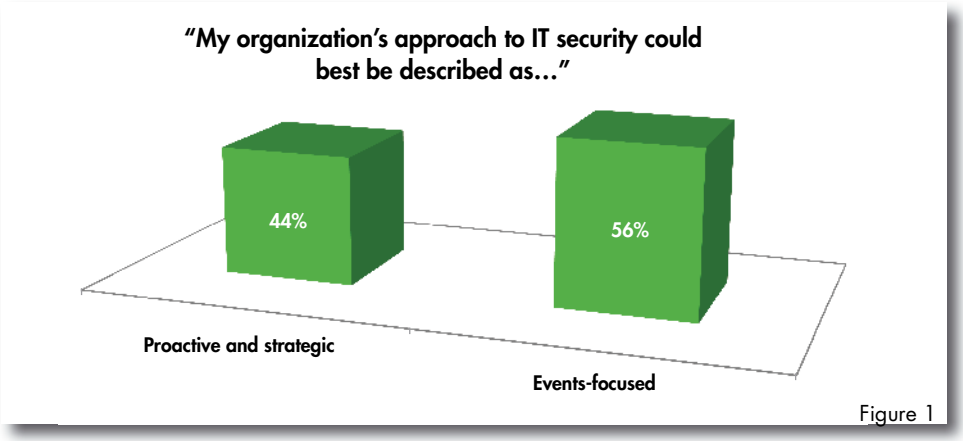

Figure 1

This approach may reflect confidence that the threat levels are low and actions taken to date are sufficient for the market environment in which Danish companies operate. Or it may be that survey respondents are expressing a concern that their firms are taking these threats too lightly.

A manufacturing CIO said, "Our organization is events-focused in its approach. It's a reflection of the level in the organization at which IT security is set. In our organization, IT security reports to line management. If we want a more proactive and strategic focus, we also need to pull it out of daily business and have it report to the Board of Directors."

Asked what the likely trend was in spending at their companies on IT security, a slight majority see investment rising moderately over the next 24 months, while 44% see that investment remaining at current levels. One respondent projected a sharp decrease in IT security investment. Please see figure 2 below.

Figure 2

"I think companies – on the business side – have made a calculation that wherever you are dealing with human behavior, it makes sense to err on the side of trust,"

one food processing industry respondent said in an interview. "To really secure our data comprehensively, we would have to really lock everything down, and as a result our business agility would suffer. On balance, companies would rather take the risks. The CIOs understand the risks and would gladly take on the job of reducing those risks – at least providing the necessary training. But the executives on the business side of some companies have given up."

DIRECT EXPERIENCE

Respondents to the survey say their companies are aware of and concerned about the incidence of hacks and other security breaches in other markets, but appear to feel relatively safe from such threats in Denmark. The country is hardly immune to such exploits, witness Se og Hør's Tys Tys case and the events involving CSC, but there have been few other publicized incidents.

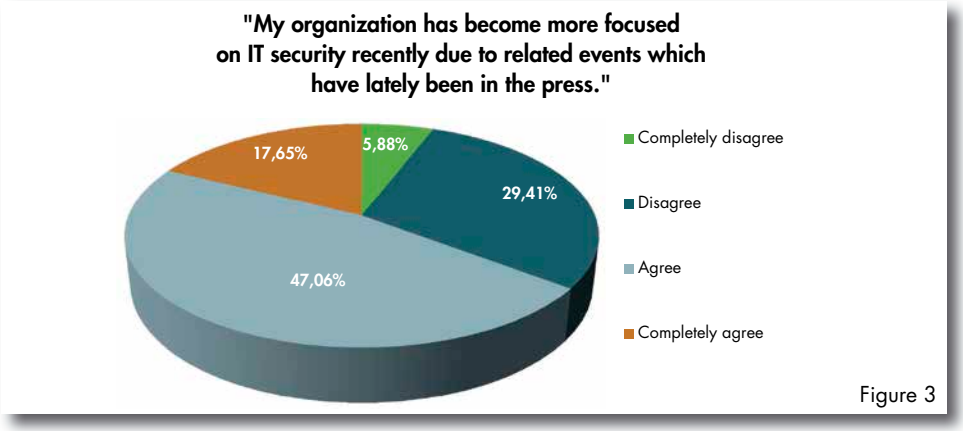

Figure 3

The survey may suggest Danish companies have been complacent, but it may also be that their own experiences bear them out.

Figure 4

Asked about their companies' own direct experiences with security breaches over the past 18 months, most organizations had had some incidents but have not seen them grow in frequency; some have seen actual declines in the incidence of breaches. Fewer than a quarter reported an increased incidence.

Respondents are influenced, however, by media reporting about security breaches. Participants in the study were asked whether they agreed or disagreed with the following proposition: **"My organization has become more focused on IT security recently due to related events which have lately been in the press."** About 65% agree or completely agree.

"We are beginning to hear more companies, including more Danish companies, come out and admit that they have been attacked," a technology industry respondent said. "But the cases of self-reporting seem to reflect loss or breach of corporate data not private or personal data. I think that says more about what companies are willing to acknowledge than what they are actually experiencing."

"Maybe there have been more attacks on Danish companies than we know about," a colleague from the finance industry opined. "If it has happened, that would be an affront to Danish pride, and I suspect there would be an effort to sweep it under the carpet rather than report it openly."

EXTERNAL DRIVERS

It is apparent that the impetus for both a concern about IT security issues and investment in IT security – tools, services and manpower – are driven more by external forces than by internal policies or concerns. One of the most important external drivers is the likelihood of stronger regulatory scrutiny of firms' security practices, anticipated in 2015 both in Denmark and across the EU.

Respondents were asked whether they agreed or disagreed with the following proposition: **"Private data regulations expected to be introduced in Europe during 2015 (i.e. General Data Protection Regulation) will require my organization to substantially change its approach to data and IT security."** More than 3/4 agree or completely agree.

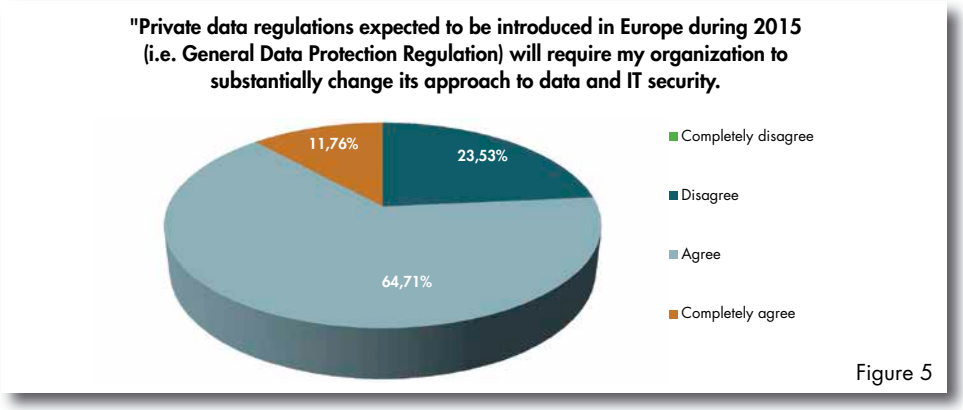

Figure 5

On the following proposition: **"Financial penalties for failure to report data breaches will make my organization more sensitive to issues of IT security and data protection,"** once again more than 80% agree or completely agree.

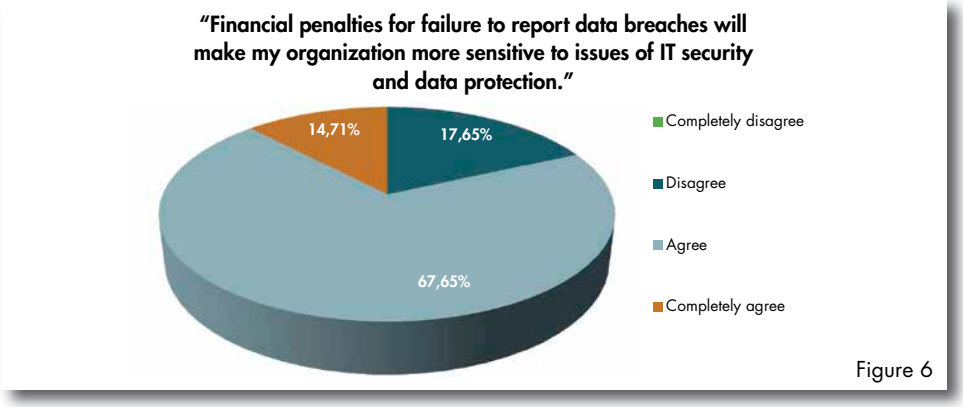

Figure 6

It seems apparent that respondents feel their companies do respond when they feel threatened with the prospect of regulatory or legal sanction – especially fines – for non-compliance with regulations, even if they are less concerned about the actual consequences of a data breach. In particular, one food industry executive noted, companies need to establish standards across all subsidiaries, including smaller subsidiaries outside Denmark.

There are skeptics, however. "I don't see how you can enforce a law that forces me to admit that we were hacked, if that is not already public information," a respondent asserted. "I don't think these regulations will have much direct effect." He added that the regulations are fundamentally aimed at consumer protection – mostly concerned with companies' protection of customer data, as opposed to the companies' own IP.

NATURE OF THREAT

What sorts of IT security threats have respondents actually experienced, or do they anticipate? The survey asked each respondent to choose the two most critical types of threats from a list.

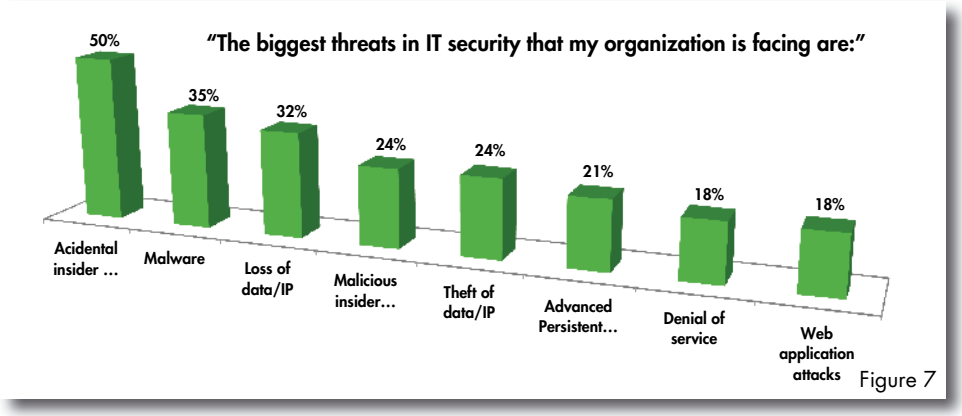

Figure 7

While their responses were fairly evenly distributed across a variety of issues, the most common concern, named by half of all respondents, was "Accidental Insider Threats" – errors and other unintentional acts by their own employees that left their operations vulnerable to data breaches.

This issue is distinct from deliberate, "Malicious Insider Threats," where employees purposely steal or destroy sensitive company data, which 24% of respondents listed as a concern. (In interviews, a manufacturing industry respondent allowed that his company had experienced several such incidents in the last 12 months.)

About 35% of respondents expressed concern about Malware; 32% listed "Loss of Data/IP" – an issue distinct from the actual "Theft of Data/IP," which 24% cited. These choices coincide with a noticeable pattern among respondents: Danish companies appear to place a generally high degree of trust in their employees, or at least their employees' loyalty and intentions, if not entirely in their competence to protect company data. (More on this pattern in the next section.)

So what are companies doing about these perceived threats? More specifically, where are they investing their IT security budgets in the coming year? Respondents were asked what the "critical IT security focus areas" for their organizations would be in the next 12 months. (They were presented a list, and allowed to choose as many as applied.)

The number one target investment was "Identity Management" (71% of responses), reflecting a concern about unauthorized data access by individuals (though not necessarily with malicious intent).

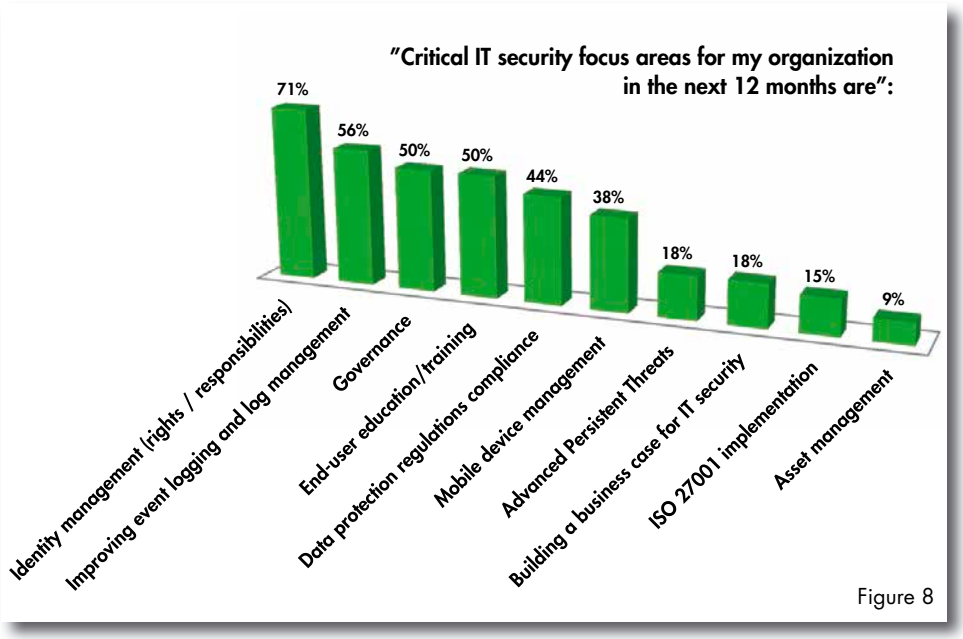

Figure 8

The next most common is investment in improved Event Logging and Log Management, intended to make breaches more traceable. Many of the most commonly cited investments are not in technical solutions, but in development of security policy and Governance, and in employee training. "Building a Business Case for IT Security" – in other words, working to bring management around to agreement to more funding – is a priority for 18% of respondents.

"Most executives, when you engage with them about IT security threats, are picturing a 'drive-by' attack by a Russian teenager who has built a virus and is now thinking, 'OK, who can I hit with this?'" an industrial materials industry veteran suggested. "But recently, we have seen an increase in more targeted attacks, more serious attempts to disrupt operations and steal data. This is what we should be worrying about, but the business doesn't quite understand this yet."

One additional driver of increased concern about security that came up in post-survey interviews is the move to cloud-based applications and data repositories, which business executives tend to perceive as less secure than on-premises systems. "We experienced a heightened awareness of these issues when we made the move to Office 365", a respondent from the manufacturing industry noted.

TRUST IN EMPLOYEES

As noted above, survey respondents display a strong pattern of trust in their employees. "We've reached a high degree of trust, and people are loathe to do anything that would be seen as an implicit breach of that trust," one transportation executive explained in a follow-up interview. However, the companies involved in this study say that they take precautions with respect to employee access to sensitive data – 59% of respondents say their companies monitor employees' access to data – a majority but not an overwhelming consensus.

One of the study's CISOs from the financial industry noted "It's so easy for one of our employees to download data and just walk out the door with a big smile on their face. We don't want to be Big Brother but we have to acknowledge that so much of this data is vulnerable to skilled IT workers."

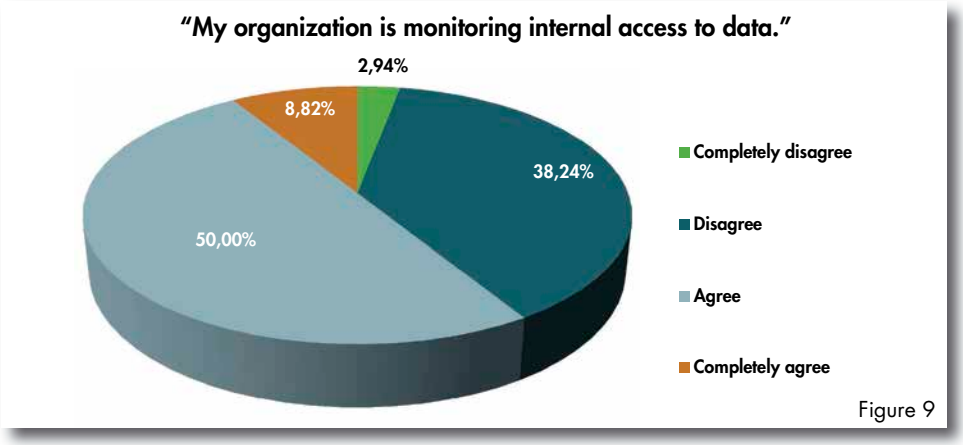

Figure 9

But Danish companies do seem to exhibit a degree of confidence that their employees can be trusted not to behave carelessly with passwords. Asked to evaluate the suggestion that employees at their organizations "would never give out a password to anyone over the phone or email," half agreed or completely agreed. "Social hacking" exploits, in which cybercriminals persuade individuals to divulge confidential information by impersonating peers or supervisors who would ordinarily be entitled to the information are common types of security threats.

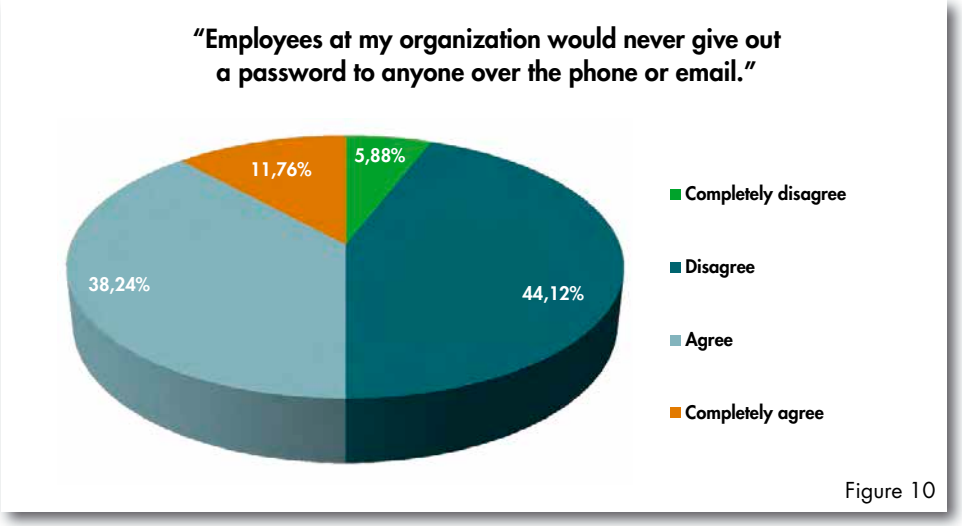

Figure 10

Figure 11

There are of course ways to test this vulnerability. Many organizations probe their own IT security defenses, contracting for deliberate hacks on their own systems to find the weaknesses. The survey asked respondents whether they employ such techniques, specifically testing their employees' susceptibility to social hacking. Only 9% of respondents said they do; interestingly, these were not necessarily the respondents who questioned their employees' ability to resist such techniques.

"We've come to the realization that we can't effectively train our users to resist social hacking techniques, because our users are so diverse and we don't control them," the transportation executive explained. "We've had to go the systems route instead and put up our defenses that way. So far it's worked pretty well. We've only had one incident in the last 18 months."

Respondents were asked whether their organizations allowed access to cloud-based file sharing solutions that their IT departments do not support, such as DropBox, OneDrive, and SlideShark. About 38% allow this – again, a minority, but not an overwhelming minority.

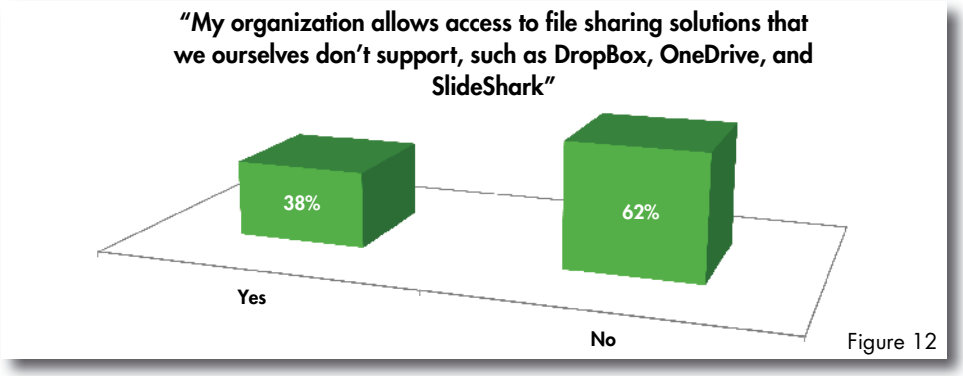

Figure 12

However, one of the CIOs from an organization that ostensibly denies access to these applications says, "In reality, we can't stop it. People need to be able to share files and they can't send big attachments to most places so, we are in the process of setting up alternative file sharing mechanisms."

RESOURCE COMMITMENT

Our research explored the nature of the manpower commitment Danish companies make to specific elements of IT security, as opposed to trusting employees to

manage their own security, depending on software tools for management of rights and credentials, or outsourcing security. On the whole, respondents indicated their companies are committed directly to staffing for security.

Figure 13

Asked whether IT staff includes "personnel responsible for managing privileged accounts," over two thirds said yes.

One CIO noted that their experience managing privileged accounts has shown that "although it's hard to get access, once given, that access is infrequently taken away later due to a job or responsibility change."

Another essential security responsibility is event logging and analysis – a function that is offered as an outsourced service to enterprises by numerous providers. But 74% of respondents indicated that they provided this function internally, using their own resources.

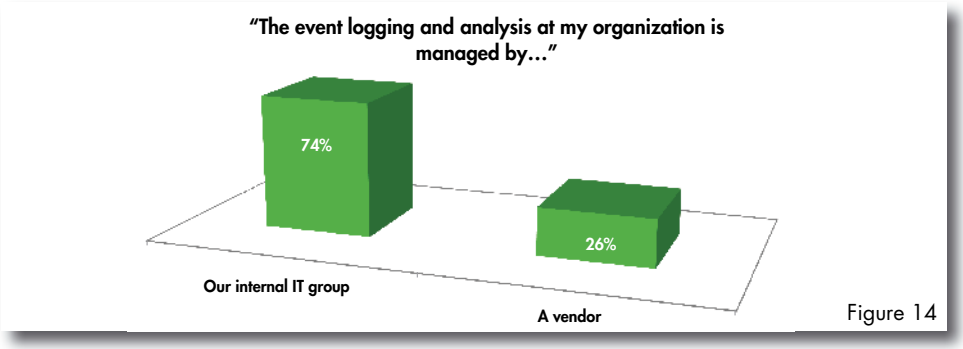

Figure 14

A manufacturing CIO ventured, "Incident logging can be critical data input for predicting and preventing attacks and loss. My company will be stronger if we're the ones managing this because we're the ones that know what the priorities are." Although ideally, "we would have some external input on events because if we are only ever seeing the events in our system, we are not getting exposure to other and newer kinds of events which makes it much harder to fix, if and when we do eventually experience them."

One other vital link in the security chain is employee training in data security best practices.

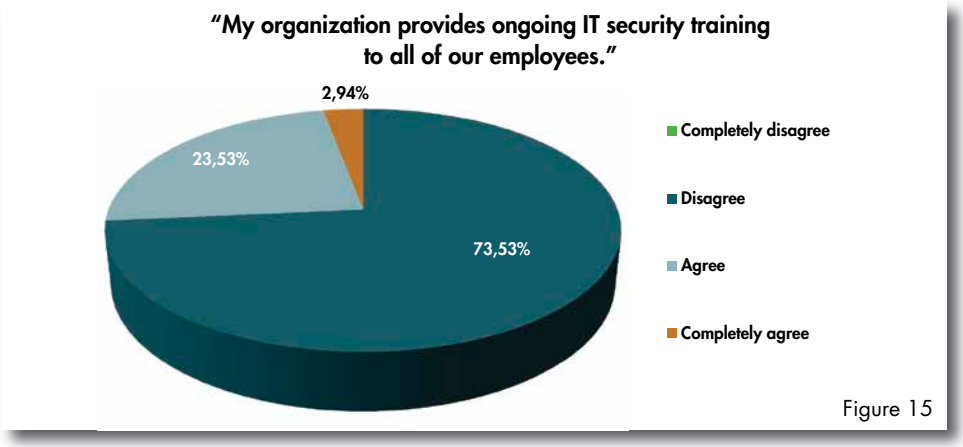

Figure 15

We saw earlier that 50% of respondents indicated training is a high priority area of focus for the coming year. But only a little over one quarter say their companies now provide ongoing IT security training for all of their employees. A CIO from the transport industry noted ironically, "It's odd that we're not training all of our employees in IT security practices. We put all of our drivers through training courses that include specific elements of IT security but that's it. They are better trained in IT security than most in our firm."

MONITORING

In addition to specific initiatives, interventions and upgrades, both to tools and procedures, effective IT security requires regular or continuous monitoring of business processes, credentials and permissions. Several questions on the survey explored companies' commitment to monitoring.

Employees are entitled to access to secure systems and data by virtue of their roles in the organization. But roles change. About three quarters of respondents indicated that they have procedures in place to regularly reviews and adjusts employee data access permissions based on their roles in the organization.

A manufacturing CIO said, "Our identity and access management practices are in the process of improving. The biggest change we have made is to start to regularly review them while also making them time-limited and/or tied to a role rather than just granting access and letting it run indefinitely."

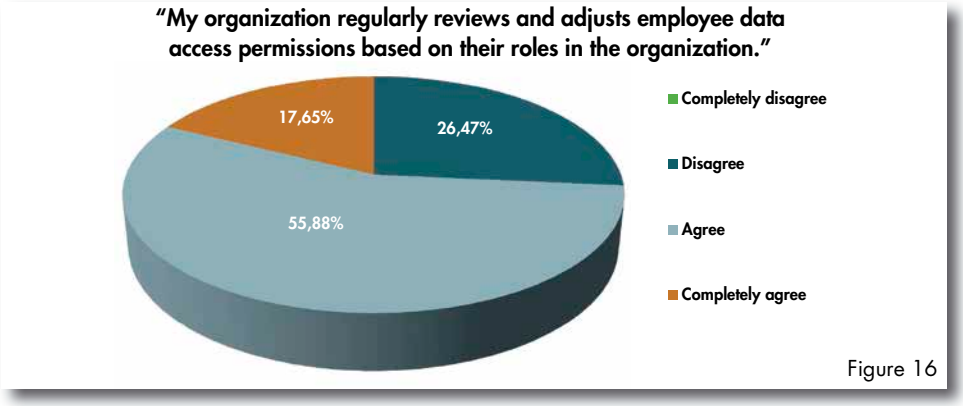

Figure 16

The survey asked whether security audits at the respondent's organization include physical access to facilities. About 82% agree or completely agree that they do.

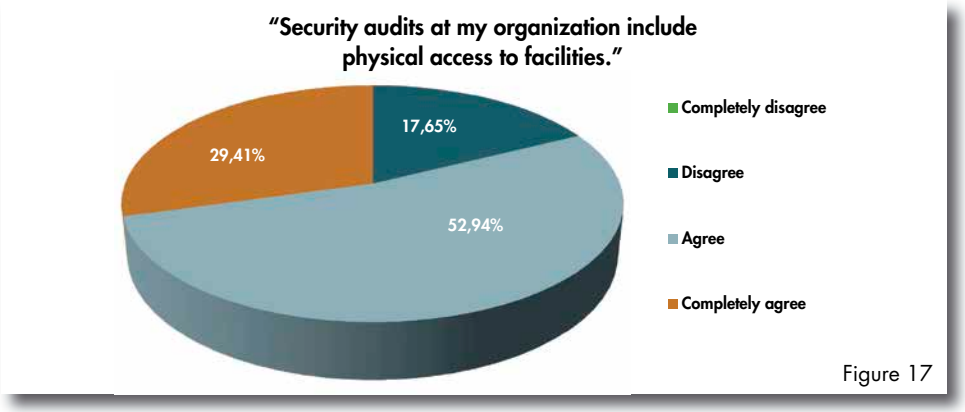

Figure 17

One CIO from the finance sector said, "There has been a big focus on physical security in our industry over the past ten years. We're definitely more mature about this than we were back then."

Almost 80% also agreed with this characterization: "As part of our IT security work, we regularly test and update our technical recovery plans to ensure business continuity in the event of a major interruption of service."

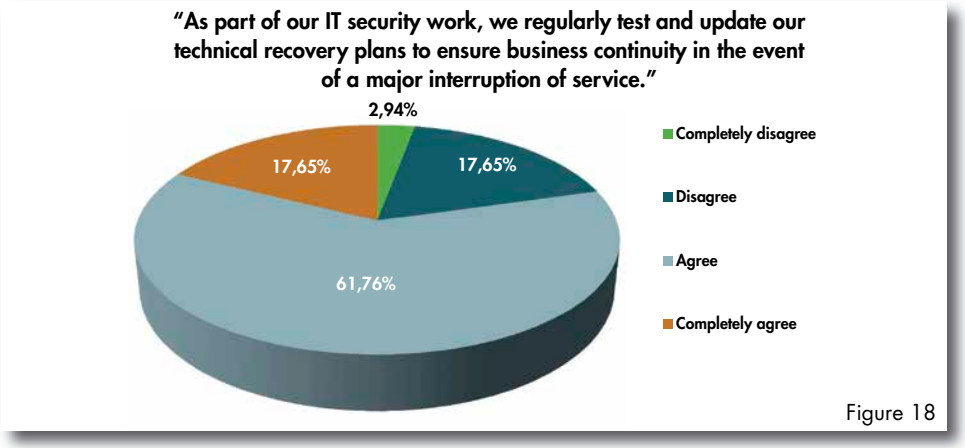

Figure 18

Although "this focus on recovery from interruption of service has muted the need to prepare organizations to recover from lost or stolen data, attacks, and other kinds of threats," notes one CIO, most respondents appear confident that the routine elements of IT security are in place, even if they separately express reservations about their companies' commitment at the strategic level.

EXECUTIVE INVOLVEMENT

IT security cannot really be said to be a strategic concern if it is never discussed at the executive level. But more than 70% of survey respondents indicated that security is indeed an executive level topic in their enterprises. "Security decisions almost always involve a cost-benefit analysis, and that has to be discussed at the executive level," one food industry respondent said. A colleague from the finance industry related that his management had eliminated a dedicated IT security role from the IT organization several years ago, but expressed optimism that it might be restored this year as security concerns grow.

Figure 19

"Classification of our data is a major priority," a manufacturing industry respondent said. "We have begun by prioritizing protection of data which we have given the highest-level classification. I suspect, though, that we will never finish formally classifying all of our data. We are in effect saying that our data in the lowest-level classification will, by default, be considered public information.

Respondents are more ambivalent, however, about the way in which IT security is discussed and assessed in the executive suite. For instance, when asked whether their companies actually track and assess their investments in IT security, slightly more than half disagreed or completely disagreed.

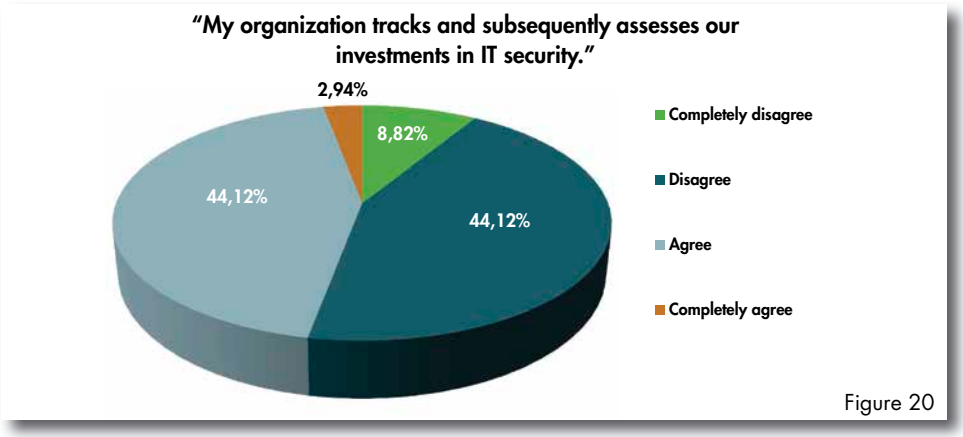

Figure 20

The naysayers' majority was slight, but it was among the individuals who had the strongest opinions about this question.

Perhaps most importantly, almost two thirds of respondents indicated that their organizations see "IT security as a cost as opposed to a value-investment."

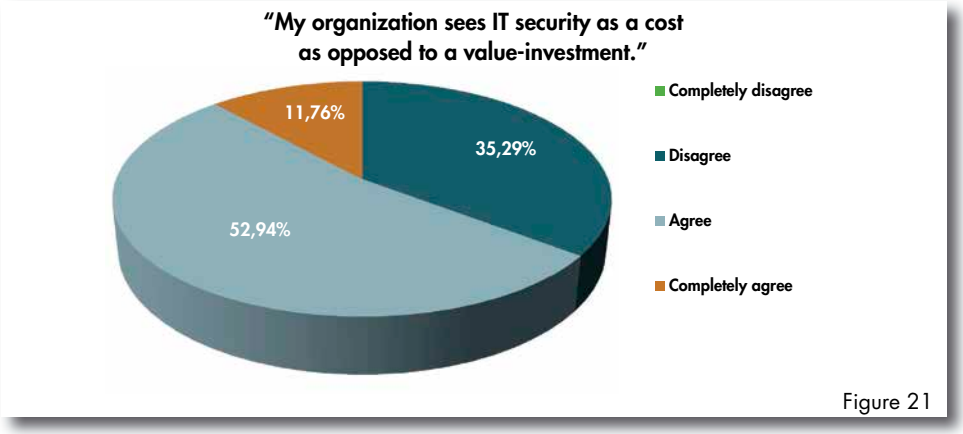

Figure 21

This is a telling indication that a significant proportion of Danish executives view the possibility of data loss or compromise as a secondary concern – an aspect of compliance – and not a genuine strategic business issue. "Let's say the IT spend at a company is 3% of the budget," a food industry respondent said. "In that case, the executives feel it is worth 3% of their attention, and security is no different."

"I like to try to position security as health insurance for the business," a colleague from the finance industry suggested. "You hope you never actually have to use it, but the value to the business is that it's there if you need it."

IT COMMUNICATION

Respondents to the survey, many of whom have personal stakes in increasing their companies' awareness and concern about security, expressed high confidence that their IT organizations can bring their executives around on the issue.

Asked to evaluate the statement "My IT organization is able to communicate on business terms with our CxO leaders so that our organization truly understands the business value of IT security," 82% agreed or completely agreed.

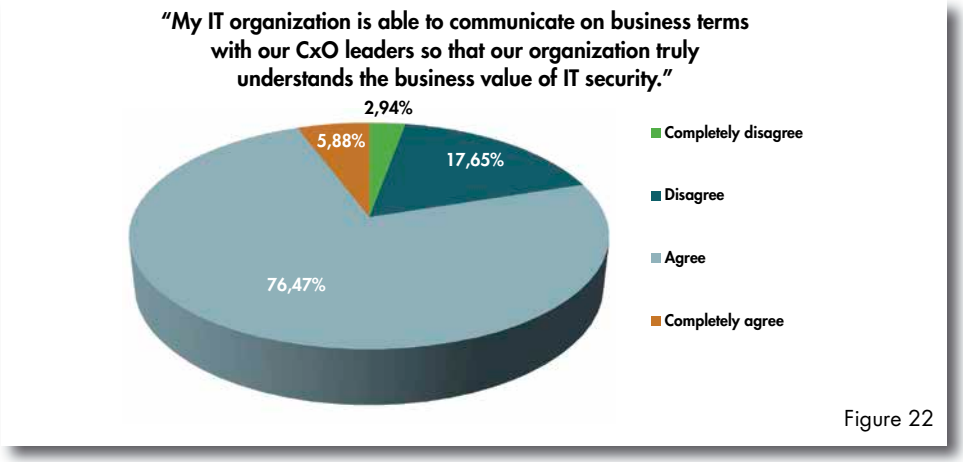

Figure 22

"I would estimate that I've spent 25% of my time educating the business on IT security over the last several years," one respondent noted. "One of the difficulties is in getting the business to understand that what was great five or ten years ago isn't state-of-the-art today."

But just what would it take today to really focus executive attention on the importance of security? Respondents were given the opportunity to express this as they saw fit. A remarkable 26% chose not to answer this question at all – a reflection, perhaps, of some frustration at the past casualness of executive attitudes toward data breaches. Of those who did answer, 9% indicated they already had executives' attention on security issues.

The more specific answers fell into several categories. About 24%, the largest group, felt management would begin taking IT security seriously when their own companies were hit by a damaging, high-profile data breach. They described this event variously as:

- "Serious data loss";
- "Loss of IP data";
- "To be declared non-compliant on regulations as laid down by the Danish FSA";
- "A smoking gun"; or
- "A major incident, or that the chairman directly requests it."

About 21% expressed the idea that executive grasp of the seriousness of security issues would come with a sort of organizational maturing – "Acceptance of "the flip side" and risks that are related to every business initiative"; "transparency in IT work"; "Awareness"; "Understanding the topic"; or "that it is seen as a strategic value on executive level."

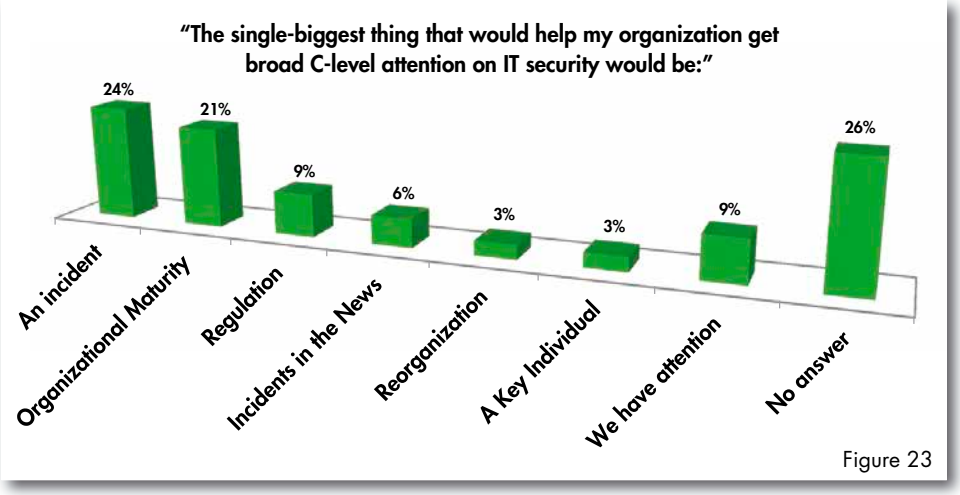

Figure 23

About 9% of the respondents in this study said the key driver for executive awareness was the anticipated Danish and EU regulations along with the threat of sanctions for noncompliance. 6% felt media coverage of large-scale breaches would bring the executives around.

"IT security should be part of a governance group, outside the control of any specific line manager, perhaps reporting directly to the Board of Directors," one respondent suggested. "Every time I make a request for funding for security, the business compares it with all the other requests that have to do with driving the business, and because they see everything related to IT as an overhead cost, security doesn't get the attention it needs."

CONCLUSIONS

Danish companies have been complacent about IT security issues, with C level executives generally remote from IT concerns and unconvinced that security is a significant threat to productivity or competitiveness. They tend to perceive the Danish market as small and relatively isolated from the intense global competition that has attracted cyberthreats in larger markets. They clearly see spending on data security as a cost to be minimized, rather than a value investment.

This complacency is being shaken by external forces – external to the individual companies and external to Denmark. There are object lessons from what has happened in other countries and many of these have gotten large-scale press coverage. But more important to Danish executives are the new regulations in the EU, and in countries where Danish companies operate, which could create serious compliance exposures and result in major fines. Danish companies seem much more concerned about legal, compliance and regulatory consequences than they are about the actual loss of data.

Executives' direct experiences – or at least what they report – would on the surface seem to confirm their attitudes. Most don't see a growing threat of security breaches and have not seen actual incidents increasing. However, more than a few interviewees note that Danish companies may be kidding themselves about this. It may be that incidents are increasing in frequency but not being reported, for fear of negative publicity – another significant fear among Danish companies that seems to supersede the concern about actual data loss. Arguably a major, highly-publicized breach in Denmark would do more to increase investment in IT security than anything else.

Data suggest that Danish managers place a high degree of trust in their employees – trust that they can be relied on to protect data and look out for the interests of the company. The prevalence of "accidental internal threats" suggests this trust may be an outdated notion.

Danish executives who have worked abroad in countries where IT security threats are taken more seriously have brought these concerns home and are among the voices bringing attention to the issue. Survey data suggest IT execs are confident in their ability to communicate the importance of security to the business leadership, but in interviews they sound less convinced of this. They are looking for a way to get the business to see the threats in tangible ways, but have not yet found the best way to do that.

Technology trends may give them an opening. The move toward more applications and data in the cloud may provide an occasion for some companies to see the need for greater protection for their data.

A high priority for IT execs who are concerned about the state of security in Denmark is to get the business to involve itself in IT security – "IT security prioritization has to come from the business," a respondent asserted. "If IT alone tries to dictate these things, it isn't taken seriously and doesn't work. It has to be seen as a bottom-line business benefit."