LegalWeek

THE AMERICAN LAWYER

In cooperation with:

CMS

Law . Tax

The Cybersecurity Challenge in Central and Eastern Europe

Are multinational companies prepared?

Risk, Resilience and Reputation

NOVEMBER 2018

Contents

This report seeks to examine how businesses operating in CEE are responding to these assorted cyber threats, what levels of risk awareness and planning they have, and where ultimate responsibility lies within disparate organisations. Legal Week Intelligence (LWI) and CMS surveyed 100 respondents from across the region. Prominent general counsel in CEE were also interviewed extensively about their cyber strategy, as well as their planning and response mechanisms, in order to determine precisely what they think and to provide greater clarity.

These interviews were conducted across a spread of jurisdictions: interviewees inevitably share many of the same concerns, although their appreciation of risk and strategies for mitigation can vary, reflecting the unique approach and structure of each business. Beyond how they do things differently, this report also seeks to address their current response to the cybersecurity challenge and how this may shape their ability to be better prepared in the future. In speaking for many of his counterparts, one survey respondent summarised the day-to-day challenge: "Cybersecurity defence is a permanent task for the company."

Introduction

Most CEE economies are thriving. Following the protracted regional downturn, a sustained recovery has led to robust growth becoming the new normal. Allied with the consequent expansion in corporate activity, the increasing complexity of CEE business operations and their developing international reach, cybersecurity is now one of the most pressing concerns affecting not only general counsel, but also boards of directors.

Cyber risk knows no borders, and the urgent need for comprehensive and effective cybersecurity is uniform in every country, although there are particular dynamics in play relating to geography and politics that make CEE particularly at risk. Multinational companies have become well attuned to the specific risks of operating in the region.

> "Every year we have more and more cyber attacks, which are more and more sophisticated – this is the challenge. It is a challenge that faces successful businesses across every country not only in the region, but globally: how to mitigate diverse threats from a spectrum of cyber risks that continuously evolve, potentially exposing corporate and customer data, thereby making it vulnerable to compromise."

Slawomir Chmielewski
Compliance & Security Director at Orange in Poland

Being Concerned, Being Prepared

The majority of respondents are manifestly concerned about the threat of future cyber attacks – no surprise given that, between them, they recorded 113 separate cyber incidents last year, which affected every one of the 18 CEE countries listed. Twenty six incidents resulted in government or regulatory action, or in subsequent litigation. Jurisdictions with the highest number of incidents included: Romania (14) Czech Republic (11) and Hungary (8). Yet from all 113 examples, not one respondent expressed dissatisfaction with their organisation's handling of the incident(s) by senior management: 54% were very satisfied and 36% were somewhat satisfied, with 10% being neutral.

According to Andrea Simandi, European data protection attorney at Microsoft, "Every CEE country thinks that they are very special and very different, but once you engage in deeper conversations to understand their concrete requirements and concerns, they are not that different. Cybersecurity has now become a CEO and GC level issue: it is so important that the leadership and boardrooms of CEE companies realise that cyber threats are for real and require effective measures to protect against. In general terms, the CEE countries are, unfortunately, still far behind Western Europe – and I hate to say that because I am from Hungary."

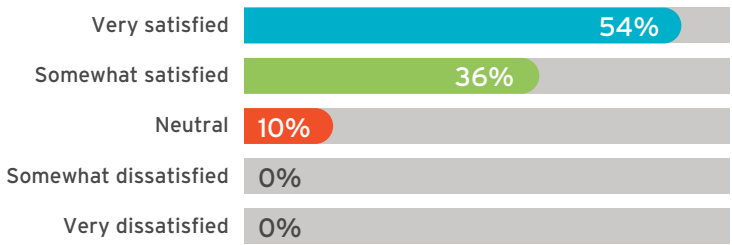
Lukasz Bendkowski, corporate counsel at Xerox in Poland, concurs: "There must be an appropriate corporate culture in place. If the board pays appropriate attention to it, then managers will follow."

Michaela Jandova, general counsel at Deloitte Central Europe, who has responsibility across the region, adds that, in terms of the level of cyber

"Every CEE country thinks that they are very special and very different, but once you engage in deeper conversations to understand their concrete requirements and concerns, they are not that different. Cybersecurity has now become a CEO and GC level issue: it is so important that the leadership and boardrooms of CEE companies realise that cyber threats are for real and require effective measures to protect against."

Andrea Simandi
European Data Protection Attorney, Microsoft

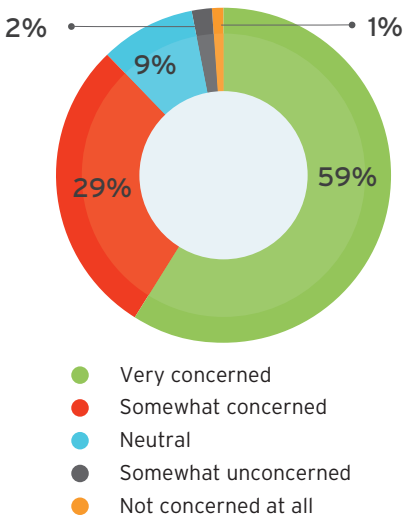
How satisfied were you with your organisation's management and response to the event?



awareness, "I do not see that much difference between the Czech Republic and Poland or Hungary – these countries are on a very similar level."

Those respondents who express concern about an attack (88%) are either very concerned (59%) or somewhat concerned (29%). There is a stark contrast, however, between these high levels of concern and how prepared they believe themselves to be for future cyber incidents: only 36% think that they are very prepared while 10% are somewhat prepared.

How concerned are you about the potential consequences of a cyber incident?



10% openly acknowledge themselves to be somewhat unprepared.

For those businesses which have already suffered attacks, the impact is often a wakeup call. One regional head of cyber security for a multinational group with operations across CEE said that 2017 was a dark year for their company, having experienced three significant incidents, each of which had some impact. This was a moment of truth for the company, as everyone involved had to look in the mirror at their preparation level. There was no adverse financial impact; however, lessons were learnt.

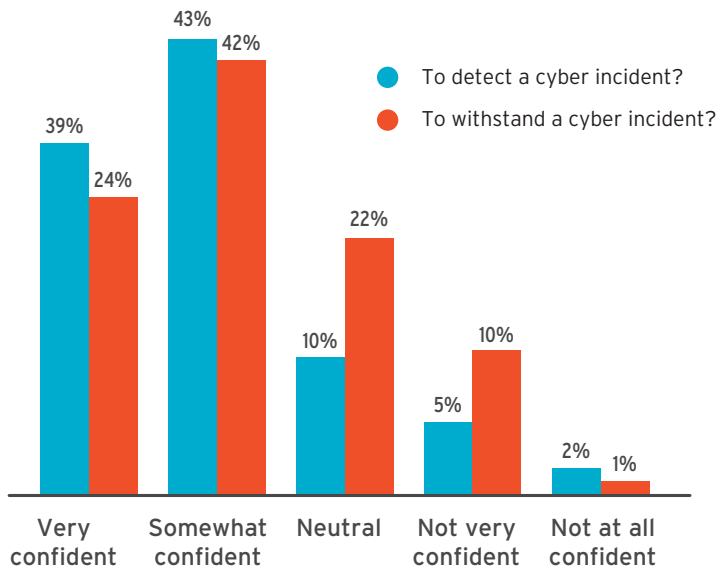
E.ON in Hungary had a better time of it, according to Peter Ban, head of legal and compliance: "We had a cyber attack relatively recently – a hacking attempt," he says. "I was quite proud reading the report and doing the follow up. It worked very well: quick reaction, quick response, an investigation, counter measures were implemented and fortunately, no evidence of any harm done."

Bendkowski observes that Xerox has also become wiser through experience. "We have had many attacks recently from China because they are trying to steal commercially valuable data."

Nevertheless, confidence levels in the ability to detect or withstand a cyber attack are conspicuously low. Only 39% of respondents are very confident in their ability to detect one, while 43% are somewhat confident. In terms of withstanding an attack, the very confident figure is even lower at 24%, with 42% being somewhat confident.

Culture and education routinely play a critical part. "Cybersecurity awareness level is quite low in Hungary," confirms Balazs Fazekas, legal and regulatory director at Invitel Group, a major player in the Hungarian telecom and information market. "Among small and medium size enterprises, it is very low. In big domestic companies and multinational companies, the awareness level goes up, but is not at the right level. As legal director at our company, I am in a unique situation, as

How confident are you in your organisation's ability:



we have a network monitoring unit professionally dealing with cybersecurity threats and incidents, so I am not really involved in cybersecurity incidents, except when they are GDPR privacy related."

Zsolt Fabian, group legal vice president at MOL Group, the Hungarian oil & gas company, the second largest company in CEE by value, adds: "My impression is that our cybersecurity team, together with our IT team, are very well prepared. I see when they operate and the results that they produce, but I can't really judge more than that; I am a lawyer."

"Cybersecurity awareness level is quite low in Hungary. Among small and medium size enterprises, it is very low. In big domestic companies and multinational companies, the awareness level goes up, but is not at the right level."

Balazs Fazekas
Legal and Regulatory Director at Invitel Group

Training & Incident Response Plans

Beyond ensuring that each system is sufficiently robust, and that the most relevant security is in place at every level, the methods for preventing cyber breaches and limiting damage when they occur are distinctly human: extensive training of employees and carefully formulated incident response plans (IRPs).

If prevention is the best deterrent, then comprehensive cyber training is essential. Microsoft's Simandi argues that it also needs to be continuous. "We have a lot of mandatory training, including on cybersecurity for all employees," she says. "This includes the explanation of how our cybersecurity is built and constantly evolves, e.g., how our internal 'red teams,' consisting of designated Microsoft employees, are trying to hack our systems to detect vulnerabilities and internal 'blue teams,' consisting of designated employees working to defend against these attacks. The conclusions of such exercises are all built in to our products and services, as well as trainings. If you are an international company without this in your core business, it's really hard to do it yourself," she says.

Orange in Poland does training on "a risk based approach," explains Chmielewski. "We divide Orange business units into categories and assess the risk of being a potential victim of a cyber attack. Then we focus on the results of this risk mapping and apply it to the appropriate frequency of training."

Meanwhile, Bendkowski suggests that "The weakest link in the chain, is always human error – something that seems very easy to address, but it's not. If you are not regularly educating staff, giving them real life examples, drawing their attention to cybersecurity, then they are open to phishing attacks, such as clicking on inappropriate emails. One person in the company may become a weak point infecting the whole IT environment. You might spend a fortune on the appropriate infrastructure, but if there is one unaware person it can destroy the whole security system."

Just over 60% of respondents have mandatory cyber training in place for employees – typically undertaken and reviewed annually – leaving almost half of them to their own devices.

"I am not satisfied with the level of training that we have," says Invitel's Fazekas. "So I will encourage my colleagues to come up with a training plan. We need to introduce training tools for the staff, including very basic things: how to avoid phishing emails, what to do with your computer – not to take it to outside places and not to leave it open – and help them understand why antivirus software is running, why they cannot just put in any USB device they want."

"The weakest link in the chain is always human error – something that seems very easy to address, but it's not. If you are not regularly educating staff, giving them real life examples, drawing their attention to cybersecurity, then they are open to fishing attacks, such as clicking on inappropriate emails."

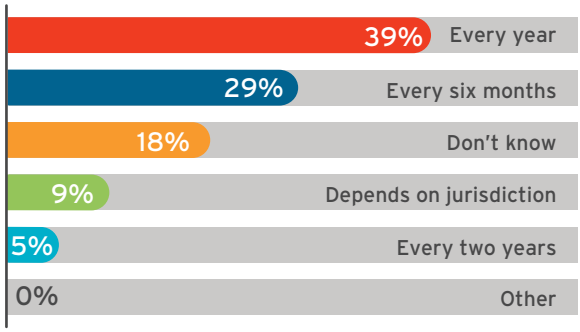
Lukasz Bendkowski
Corporate Counsel at Xerox

But even when proactive senior management ensures that appropriate training systems are in place, problems still exist in developing routine cyber awareness and in establishing protocols that employees will automatically follow. "You can see it even among our own staff," says Deloitte's Jandova. "Even though we have regular training, you have to push really hard for them to focus and to prioritise – security, privacy or cyber."

Should the worst happen, the other arm of being prepared is having an up-to-date IRP in place that enables a breach to be contained and the damage limited – insofar as this is possible. IRPs have a similar level of adoption to training: 68% of respondents have a different IRP for each CEE country in which they operate. Of these, 39% of respondents update them annually and 29% every six months, while 18% do not know how often they are updated. Ownership of the issue is not always at the forefront of respondents' thinking, and understandably, most are reluctant to discuss the details of their response plans.

Do you have an incident response plan (IRP) for each CEE country in which you operate?

How often are your IRPs updated for each CEE country in which you operate?



"Since I have been here, the IRP has not been reviewed, but it is quite recent. It's reviewed more or less annually. I don't think it needs any review right now, but I expect that some changes will need to be made," says Invitel's Fazekas.

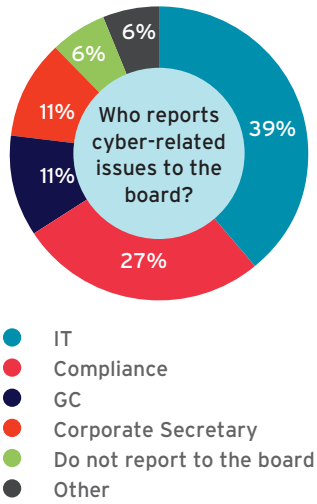
Meanwhile says Fazekas: "We have an IRP, and also a review – if anything is identified, of course, we have to react immediately."

Jandova adds: "We have everything in place including an incident reporting desk in CEE that deals with any incidents, not only cyber, but also potential data leaks and stolen computers."

Reporting, Responsibility and Regulation

On one issue, a strong consensus exists – the time spent managing and mitigating cyber risk in CEE is increasing: 67% of respondents have seen an increase in the past year, 30% say it is about the same, while only 3% report a decrease. However, the three big Rs – responsibility, reporting and regulation – produce some of the biggest divergences between companies. The more difficult questions of where exactly the buck stops and who reports what and when to the board on cyber matters have no common answer.

So who does report to the board on cyber-related issues? The question provokes a wide spread of responses: IT – 39%; Compliance – 27%; General Counsel – 11%; Corporate Secretary – 11%; Other – 6%. Perhaps the most striking is the relatively low level of GCs. By contrast, in a report published last year by Kroll in association with LWI, 27% of US general counsel reported to the board on cyber matters. In terms of how often, only 25% of respondents said that this happened more frequently than every six months, while 5% said it was every two years.



67%

of respondents report an increase in time spent managing and mitigating cyber risk in the last 12 months

30%

of respondents report their level of managing and mitigating risk has remained the same in the past 12 months compared to prior year

The highest figure – 42% – did not report to the board at all.

At E.ON, Ban sits on the board of the Hungarian holding company. "As the data privacy officer for the domestic subsidiaries, I am the person responsible," he says. "But as far as cybersecurity is concerned, we have a separate department dealing with information security from a purely technical aspect. Fortunately, both data privacy and data security are pretty high on the board agenda." Ban is responsible for cyber issues concerning personal data alongside the head of information security. "We have regular

meetings and investigate incidents jointly – it's a shared responsibility," he explains. "Most of my counterparts in other companies do not really perceive that it is something that naturally fits within the legal function, but of course you cannot avoid to think about a convergence happening sooner or later."

In terms of reporting, Deloitte's Jandova wears three hats: "I report to the chair of the board of directors, to the CEO, and I also report to the Reputation and Risk Leader," she says. For Fazekas, the process at Invitel is somewhat different. "If it is a pure cybersecurity incident, then it will be handled through the regular cybersecurity processes," he says. "But if it has a data protection angle, then I will come into the picture. Because I am also the data protection officer, I will be involved in helping to orchestrate the necessary steps after a cyber incident."

Likewise, at MOL, Fabian explains that he does not report to the board on cyber matters: "The cybersecurity team reports to the IT department that is supervised by the finance department which reports to the CFO, who would then report any problems that occur to the board. The same pattern applies in 30-plus countries where we have operations, many of those in CEE. The cybersecurity team together with the IT team also report back to the board, so the operational board and the board of directors are regularly updated on cyber matters."

Chmielewski finds it invaluable to report to the Orange board in Poland: "When there is a decision makers' meeting and we want to decide about investing more money in cybersecurity or make additional plans for cyber training, if there are questions, I can show examples of data leakage at Google, at Facebook," he says. "It is very helpful in solving organisational or financial problems, and keeping up with the appropriate applications."

By a margin of more than two to one (67% vs 33%), respondents believe that cybersecurity procedures and protocols used by regulators need improvement across the region. This is the majority view in every single CEE country. Those with the highest percentage in order: Lithuania, Albania, Ukraine, Slovakia, the Czech Republic, Bulgaria, Slovenia, Hungary and Poland. "Because we share systems within CEE, we have to keep the highest standards possible, so we can be considered as over-compliant in countries outside the EU," says Jandova.

"We [legal and information security] have regular meetings and investigate incidents jointly – it's a shared responsibility. Most of my counterparts in other companies do not really perceive that it is something that naturally fits within the legal function, but of course you cannot avoid to think about a convergence happening sooner or later."

Peter Ban
Head of Legal and Compliance at E.ON in Hungary

GDPR & NIS

In discussing regulation that impacts on cybersecurity, every interviewee spoke about GDPR compliance at length – no surprise since it consumed so much of their time and energy before the May 2018 deadline when it began to apply in every EU member state. However, only a small part of GDPR is cybersecurity related. Instead, what particularly focussed minds was the enormous potential penalties for non-compliance. A fine of up to € 20m, or 4% annual global turnover, whichever is higher, proved a compelling reason for many businesses to take data privacy seriously.

Rather less attention was paid, however, to the Directive on Security of Network and Information Systems (NIS), which also came into force at the same time. At least one interviewee had never heard of it, even though the measures it contains are specifically designed to help mitigate the risks of cybersecurity breaches in a preventative manner.

"To be honest, the focus has been on GDPR," says MOL's Fabian. "GDPR had the bigger impact; NIS was viewed more as a requirement that needs to be tackled by professional people in the organisation," confirms Fazekas. "So GDPR received more attention from the management and from the average employee."

Xerox has a hybrid compliance model, explains Bendkowski. "When there is a new EU or national regulation, we take or supplement internal guidelines to form cross-functional teams to implement and monitor our local compliance with these requirements – applicable to GDPR, or cybersecurity," he says. "With GDPR, you have 72 hours to report incidents; here you have max. 24 hours to react properly." Chmielewski expands on Orange's compliance: "The NIS directive concerns resources for a high level of common security of networks and systems throughout the EU – we are trying to meet all those requirements. In addition, our government is rapidly developing legislation regarding a national cybersecurity system, regulating all spheres of cybersecurity in Poland: it is challenging for us."

Jandova provides a broader picture: "These regulations are so complex, so technical that many people and businesses in general here do not understand them and don't want to deal with them because of the complexity. So they usually try to avoid them, unless they have internal specialists who are in charge of compliance as it is in my company. The environment here is: this is over-regulated and it cannot happen to us. Until a cyber breach hits them, then they see the need for these regulations and become very careful."

Microsoft's Simandi also sees huge variances between different countries. "Look at how GDPR enforcement has begun," she says. "Everybody was so afraid of 25th May – what would happen with data protection authorities having powers to impose enormous fines. But in reality, they are struggling with a huge number of notifications, many of which are wrongly sent emails and are not asking companies to be more thoughtful and selective in reporting, and to focus on what was really the goal of the personal data breach notification requirements of the GDPR."

Simandi continues: "Apart from a few exceptions, the situation is even worse on the cybersecurity front because the regulators are sometimes really small and are often lacking the most up-to-date technical and security expertise and resources. The way forward in CEE is to work with professionals, pick and choose what built-in security they want to leverage to ensure that the governments have secure environments in order to avoid vulnerabilities, as they are definitely in the forefront of cybercriminals' minds, as recent examples have shown. In terms of the NIS directive, an effective framework has been agreed, but governments need to implement and harmonize the framework locally, which is still missing in many countries even past the November 2018 deadline. So, it really comes down to: when it is a populist or nationalist leadership, how much they are willing to listen to their own professional advisers?"

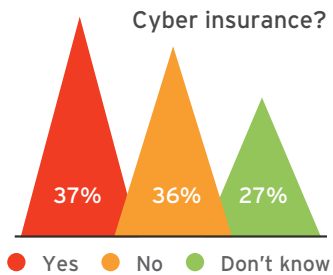
"These regulations are so complex, so technical that many people and businesses in general here do not understand them and don't want to deal with them because of the complexity. So they usually try to avoid them, unless they have internal specialists who are in charge of compliance as it is in my company. The environment here is: this is over-regulated and it cannot happen to us. Until a cyber breach hits them, then they see the need for these regulations and become very careful."

Michaela Jandova
General Counsel at Deloitte Central Europe

Cyber Insurance

Considering the widespread appreciation of cyber risk – at least among general counsel and board members – and the increasing prevalence of breaches and attacks, the current purchase levels of cyber insurance are still low: only 37% of respondents have specific cyber coverage. While uptake may lag behind risk perception, this is changing fast according to Emy Donavan, chief underwriting officer, cyber at Allianz. There is a direct correlation between company size, the sophistication of the jurisdiction and the decision to purchase cyber insurance. Buyers in CEE are therefore primarily among the largest companies, while "mid-sized companies are looking at it, but not necessarily buying yet," she says.

So how does Allianz overcome this resistance problem? "You scare them," says Donavan. "It has got to be a little bit of a shock and awe tactic. It is like the climate change report; people look at it and think: it's too big an issue, and they freeze up. But if you start talking to them about actual things that they can do to improve their risks first of all, but also things that could happen to them if they don't, then you start to tie consequences to actions: look at what happened to so and so. The more law suits that we see in the news, we can definitely say: look at what happened to Equifax, as a perfect example. Yahoo is also a really good example, especially because it affected the sale price when they were acquired – a warning for publicly traded companies."



Nevertheless, cyber insurance in CEE remains largely embryonic for most local CEE companies, argues Jandova. "Some businesses have started to look around for a quote," she says. "But the local insurance companies, including in the Czech Republic which is on the higher level of CEE countries, are not ready for it yet."

But Orange in Poland does, confirms Chmielewski. "I don't want to go into the details," he says. "But it mitigates some risks and can shift risk from the company to the insurer."

Donavan provides some overall context on the growth of cyber insurance: "From a global perspective, uptake for cyber risk is led by the US, largely because there have been mandatory notification laws in place since 2003," she explains. "Now Europe has caught up and gone a step further with GDPR. When you look at GDPR regulations, an issue that a lot of companies are struggling with is that unless you have really thought through the requirements well in advance, it is entirely possible that the systems at a given company will not be configured in such a way that allows them to comply. Also, because personal rights are now much greater, there are some significant challenges, and in some instances, there has been risk transfer via cyber insurance policies. These policies may not always be able to provide cover, depending on what fines or penalties are insurable, but they can certainly help the response to crisis management, which is becoming more of a consideration."

> "...mid-sized companies are looking at [cyber insurance], but not necessarily buying yet."

Emy Donavan
Chief Underwriting Officer, Cyber at Allianz

> The average cost of a data breach is approximately $4 million – representing a total one-year cost increase of 6.4%.
>
> **2018 Cost of a Data Breach Study: Global Overview,** *conducted by Ponemon Institute LLC, July 2018*

Conclusion

"After corruption and drugs, cyber crime is the third biggest organised criminal industry worldwide," says Dora Petranyi, partner and CEE managing director at CMS. "There is no way you can be completely protected against the cybersecurity threat," she cautions. "You cannot get a 100% assurance that everything is going to be smooth. But you can make your company resilient in terms of continuing activities, even if you are hit." Olga Belyakova, partner at CMS, adds: "No one is immune. Although risk cannot be eliminated, it can be significantly mitigated, potentially saving a business millions of pounds – and lawyers have a critical role to play in that process."

In distilling the key message from the various points made by interviewees in this report about tackling operational risk, these comments serve as a stark warning to businesses everywhere. And for those companies operating in CEE who do not yet have adequate cyber training, monitoring, planning and reporting procedures in place, it is particularly important.

Cyber may be an invisible risk, but it is also very real and, as many businesses know too well, cyber attacks cost. McKinsey recently reported that the average cost of a data breach is $4 million, without accounting for any damage to the brand's reputation or any subsequent litigation that might follow. Beyond the commercial imperative to save money, like every challenge facing business, taking cyber seriously also presents an opportunity to protect customers, shareholders and employees, to preserve the integrity of the brand and to enhance its reputation, both nationally and internationally.

The future development of businesses in CEE depends on multiple factors. For CEOs and their fellow board directors, cybersecurity may not appear critical since it is defensive by nature, rather than offensive: there is no automatic or tangible added value that can be delivered by implementing it. But the message from respondents and interviewees alike is clear: having a carefully crafted, well-executed and regularly updated cyber strategy will become integral to their future success. Without this key element, that success may be in real jeopardy.

"After corruption and drugs, cyber crime is the third biggest organised criminal industry worldwide. There is no way you can be completely protected against the cybersecurity threat. You cannot get a 100% assurance that everything is going to be smooth. But you can make your company resilient in terms of continuing activities, even if you are hit."

Dora Petranyi
CEE Managing Director, CMS

Whatever your risk, you need to deal with them in ways that builds your resilience and protects your reputation. We will be there around the clock and around the world, whenever and wherever you need us.

CMS in CEE

With more than 100 partners and 500 other lawyers across 17 full-service offices in CEE (more than any other law firm) we understand the business and regulatory landscape of the region inside out. We have been advising global corporations and investors in Central & Eastern Europe for over 30 years. Clients come to us for local insight combined with global perspective.

Our teams in CEE are top-ranked in their jurisdictions and regionally. We regularly mobilise large multi-disciplinary and multi-country teams to deliver top class specialist support to quickly respond to and tackle complex or sensitive risk-related matters from every angle, from emergency response and dealing with regulators, to disputes and data breaches.

Our CEE cybersecurity team can advise you on the full range of cyber-related matters and products to help you manage cyber risk, at board-level and throughout your business, across as many countries as you need us. Our experts can work with you from the start to diligence your business and identify any weak spots when it comes to your cyber infrastructure, as well as build and test strategic and sound incident response plans. We can be there to support during or post a cyber attack, offering full crisis management services, including dealing with regulators and enforcement response if required.

Our CEE offices

CMS ALBANIA
Based in Tirana
Established 2012
> 7 lawyers

CMS BOSNIA AND HERZEGOVINA
Based in Sarajevo
Established 2008
> 10 lawyers

CMS BULGARIA
Based in Sofia
Established 2005
> 40 lawyers

CMS CROATIA
Based in Zagreb
Established 2003
> 25 lawyers

CMS CZECH REPUBLIC
Based in Prague
Established 1991
> 40 lawyers

CMS HUNGARY
Based in Budapest
Established 1989
> 75 lawyers

CMS MONTENEGRO
Based in Podgorica
Established 2012
> 4 lawyers

CMS POLAND
Warsaw and Poznan
Established 1990
> 150 lawyers

CMS ROMANIA
Based in Bucharest
Established 1999
> 65 lawyers

CMS RUSSIA
Based in Moscow
Established 1992
> 50 lawyers

CMS SERBIA
Based in Belgrade
Established 2000
> 18 lawyers

CMS SLOVENIA
Based in Ljubljana
Established 2008
> 15 lawyers

CMS SLOVAKIA
Based in Bratislava
Established 2017
> 10 lawyers

CMS TURKEY
Based in Istanbul
Established 2013
> 20 lawyers

CMS UKRAINE
Based in Kyiv
Established 2007
> 30 lawyers

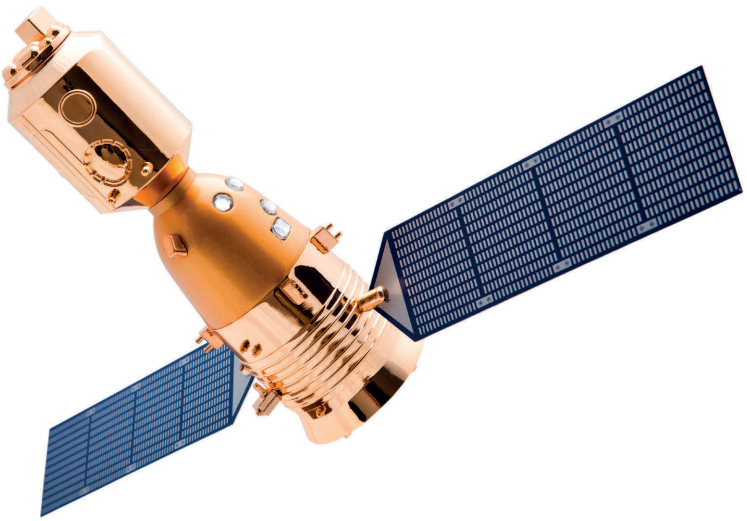
Your key contacts for cybersecurity in CEE

Dora Petranyi
Managing Director – CEE
E dora.petranyi@cms-cmno.com

Olga Belyakova
Partner
E olga.belyakova@cms-cmno.com

Risk, Resilience and Reputation

C/M/S/
Law.Tax



Risks come in many forms.

You need integrated support from a firm that has the sector expertise, the range of commercial experience and world-class teams to quickly respond and tackle your risk matrix from every angle.

CMS offers a true 360° approach, from full-spectrum long-term planning to emergency response, a responsive and reassuring support in your dealings with regulators to reporters, on issues from disputes to data breaches, in arenas from cyberspace to the c-suite.

Whatever your risk, you need to deal with them in ways that builds your resilience and protects your reputation. We will be there around the clock and around the world, whenever and wherever you need us.

To talk in more detail about cybersecurity in CEE, please contact CEE Managing Director and cybersecurity specialist Dora Petranyi (dora.petranyi@cms-cmno.com) or your usual CMS contact.

Your World First
cms.law

In association with

C/M/S/

Law . Tax

Legal Week Intelligence is the independent research division of Legal Week, part of the ALM Media group of leading business publications.

For over 10 years, Legal Week Intelligence has conducted research for global and national law firms, companies and vendors as a group or individually, under strict Market Research Society guidelines, on generic and industry specific topics. Research can be in the public domain or form part of a confidential project for individual clients on a bespoke basis. Over the years, we have reached out to thousands of associates, partners and general counsel.

We advise business leaders on their critical issues and opportunities including strategy, marketing, operations and technology. We work with leading organisations across the private, public and social sectors. We have deep functional and industry expertise as well as breadth of geographical reach.

In all cases, Legal Week Intelligence benefits from access to the industry expertise of Legal Week editors and journalists, a dedicated research & analysis team and the global reach of ALM Media and its affiliates. This enables our clients to improve the quality of their decision-making by providing them with reliable data, robust analysis and actionable advice.

We focus debate on the most important and pressing issues using scalable research products and a flexible multi-media output. Furthermore, we emphasise the conversion of our information into actionable advice and we strive to leave businesses stronger after every engagement.

ALM