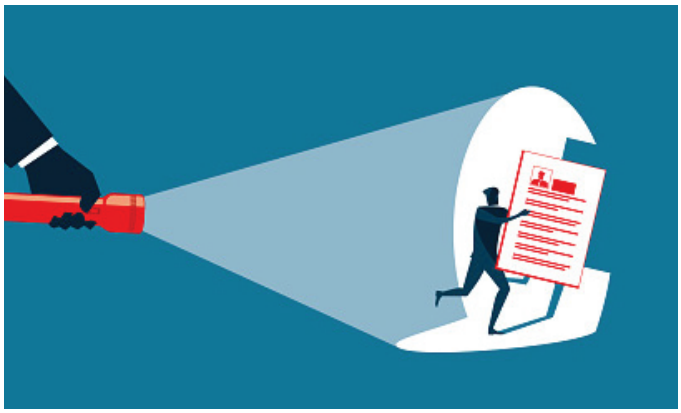
TONE at the TOP®

Предоставя на висшето ръководство, Съветите и одитните комитети кратка информация относно теми, свързани с управлението.

Брой 106 | Август 2021

Лице в лице с „чудовището“ Киберсигурност



Киберрисковете продължават да засягат организации, различни по своя мащаб и индустриална ниша, и по всичко личи, че тази тенденция ще се запази и в бъдеще. Проучване, направено сред членове на Съветите и ръководители, постави киберзаплахите на десето място в класацията на най-сериозните организационни рискове за 2021 г., като отговорилите очакват те да бъдат основен риск и през 2030 г. По данни на „Cybersecurity Ventures“ глобалната киберпрестъпност ще нараства с до 15% годишно, като прогнозите са финансовото ѝ измерение да достигне 10,5 трилиона долара до 2025 г. Компанията за киберизследвания нарича това явление „най-големият трансфер на икономическо богатство в историята“.

Кибератаките се извършват под формата на рансъмуер (ransomware), атаки срещу отдалечени работни ресурси, атаки, засягащи веригата на доставки, фишинг или посредством други престъпни практики. Те могат да спънат дейността на компания, да намалят значително стойността ѝ и да накърнят сериозно репутацията ѝ. Разходите за организациите след пробив в базите им данни са високи и продължават да нарастват, през 2021г. са били средно 4,24 милиона долара, което е почти 10% повече за една година, сочи проучване на IBM.

Нещо повече, пандемията COVID-19 създаде нови „уязвими места“, които тепърва трябва да бъдат напълно проучени или докладвани.

Управление на заплахите

Когато залогът е толкова висок, има редица стъпки, които Съветите могат да предприемат, за да подобрят надзора си върху киберрисковете. По време на целия процес вътрешният одит може да служи като критичен партньор. Работейки в сътрудничество с експертите по киберсигурност в организацията, екипът по вътрешен одит може да предложи обективно мнение за организационните планове - изпълняват ли се те по предназначение и адекватни ли са спрямо поставените задачи.

„Те могат да докладват пред Съвета дали организацията е изложена на голям риск или пък се доверява на измамно чувство за сигурност“, казва Санди Пундман, CIA, старши партньор Консултантски услуги относно риска и финансите в Делойт.

Съществуват различни стратегии, които Съветът може да предприеме, за да подпомогне справянето с киберрисковете. Пундман и други препоръчват стремеж към задълбочено разбиране относно организационния профил на киберрисковете, отговорно изпълнение на надзорната им роля и практикуване на „здравословен скептицизъм“, за да гарантират, че имат ясно разбиране както за силните страни, така и за уязвимите места на организацията.

Разпределете надзорни роли и насрочвайте редовни актуализации. По данни на проучване на „Gartner, Inc.“ днес в по-малко от 10% от Съветите функционира специален комитет по киберсигурност, ръководен от квалифициран член на Съвета, като този брой се очаква да нарасне с около 40% до 2025 г. Това увеличение може да се дължи на подема на онлайн бизнеса и дистанционната работа по време на пандемията и допълнителните потенциални рискове, свързани с тях.

Относно Института на вътрешните одитори (The IIA)

Институтът на вътрешните одитори (The IIA) е световна професионална асоциация с повече от 200 000 членове в повече от 170 държави и територии. Институтът на вътрешните одитори изпълнява функцията на основен защитник на професията на вътрешните одитори, създател на международни стандарти и основен изследовател и обучител в тази сфера.

Институт на вътрешните одитори

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

Безплатен абонамент

Посетете www.theiia.org/tone, за да се регистрирате за вашия безплатен абонамент

Обратна връзка от читателите

Изпращайте въпроси/коментари на Tone@theiia.org.

Пундман подчертава, че в наши дни е трудно да се определи кой и каква отговорност носи що се отнася до надзора върху киберсигурността, тъй като често тя е разпределена между ръководството и различните комитети. На определен комитет трябва да бъде възложена отговорност и киберсигурността да присъства задължително сред темите за обсъждане на всяко заседание. Още повече - киберсигурността следва да бъде и сред темите от дневния ред на Съвета минимум два пъти годишно.

Определяйте с точност нивото на заплаха. Киберсигурността е нещо повече от IT проблем. „Независимо дали преди или по време на атака, е нужно не просто да оставите [киберсигурността] на IT директора и техническия екип“, казва Джон Ноубъл, бивш директор на Националния център за киберсигурност на Обединеното кралство, в подкаст на McKinsey. „Лидерите трябва да решат как да управляват напрежението между използваемостта, сигурността и разходите и това е мястото, където се нуждаем да предизвикаме Съвета и от тестовите процеси.“

Внимание към детайлите. „Съветите трябва да са наясно дали тяхната организация редовно оценява и актуализира оценката на киберрисковете. На екипа по вътрешен одит често се възлага извършването на първоначална оценка или проект, може би одит на атака и пробив, но това е само първа стъпка“, предупреждава Пундман. „Организациите се нуждаят от мащабна стратегия за предотвратяване, откриване и противодействие на кибератаки. Действията трябва да включват оценка на текущите стъпки, които е предприела организацията, за да разбере атаките, ефективността на взетите мерки за разкриване и противодействие на атаки, как се проследяват инцидентите и предприетите действия, какъв е механизма на това противодействие и колко успешен е той. Оценяването на цялостната стратегия може да започне на ниво комитет, но тя трябва да бъде разгледана и от целия Съвет“, допълва тя.

Както бе отбелязано в публикация на Делойт, първата линия на защита от кибератаки включва бизнес и ИТ звената, за които рискът е част от текущата оперативна дейност. Втората линия на защита в организацията са отговорните звена за управлението на риска в областта на информационните системи и технологии, чиято задача са управлението и надзора. Функцията за вътрешен одит все по-често е третата линия, осигуряваща независим преглед на мерките за сигурност и тяхната ефективност.

Разберете какво отличава този риск. Организациите и техните Съвети са запознати с рисковете, но тези, свързани с киберсигурността, са различни по няколко причини. Първо, тя предполага специфични познания и заплахите се видоизменят непрекъснато, поставяйки ги отвъд опита на много от членовете на Съвета. Второ, използването на интернет е широко разпространено в повечето организации, така че рисковете и тяхното въздействие са многостранни и сложни. „Достъпът на организацията до интернет е от основно значение за постигането на стойност, а всички онези транзакции, които могат да се извършат единствено онлайн, по своята същност са опасни“, споделя участник в панелна дискусия между директорите по управление на киберрискове. „Това от своя страна не важи за всеки друг аспект на риска, с който се справят Съветите.“

ВЪПРОСИ КЪМ ЧЛЕНОВЕТЕ НА СЪВЕТА

- Колко често Съветът получава актуална информация относно заплахите от кибератаки в организацията и стъпките, които се предприемат за справяне и управление на киберрискове?
- Разглежда ли организацията киберсигурността като риск за компанията, а не като изключително ИТ проблем?
- Съветът играе ли проактивна роля в надзора на киберрискове или приема, че всичко е наред, освен ако не е посочено друго?
- Съветът има ли специален комитет по киберсигурност? Ако не, има ли друг комитет, като одитен комитет, надзорна отговорност за киберсигурността?

Вземете пример от реалния живот. В едно настолно упражнение, *подходящо за вътрешни одитори, мениджъри или външни за организацията страни*, Съветът и висшето ръководство могат да наблюдават симулирана атака, за да преценят как организацията реагира спрямо нея, как се уведомяват инвеститорите и по какъв начин тя засяга клиентите или бизнес партньорите. (Пундман дори е работила със Съвет, по чиято преценка единствено Главният ИТ директор (CIO) и Главният изпълнителен директор (CEO) са били предупредени, че ситуацията е симулирана, за да бъде упражнението възможно най-реалистично). След като организацията оцени отговора си, Съветът може да получи актуализация за промените, които са направени или са в ход.

Вътрешният одит може да бъде основен играч и в друго полезно упражнение: Визуализация на модела на зрялост, която дава представа на високо ниво за киберрисковете и сравнява къде организацията се справя добре, всичко от гледна точка на неспециалист. Управлението и справянето с висички рискове в организацията е трудоемко, а тези упражнения могат да помогнат да се изясни кои рискове са най-критични, така че организацията да подобри откриването им и превенцията в тези области, казва Пундман.

Не позволявайте на рисковете да ви изненадат. С увеличаващата се употреба на технологиите се увеличават и рисковете, свързани с непознати нововъзникващи технологии. Дори нова ERP система може да постави предизвикателства пред сигурността, които не бива да се пропускат, отбеляза Пундман. Много компании погрешно изчакват, докато възникнат проблеми с нова система, преди да планират как да се справят с тези проблеми. „Уверете се, че от самото начало имате план за защита на вашата стратегия за кибератичност и контрол“, казва тя.

Организациите, участващи в сливания и придобивания, също могат да се сблъскат с нови уязвимости. „Ако придобивате компания, попитайте какви рискове поемате, когато разширявате бизнеса си“, посъветва тя. Компаниите, работещи с вериги за доставки или трети страни, също могат да бъдат изложени на рискове от такива източници. В допълнение, на арената за предоставяне на съответствие, организациите трябва да са наясно със съответните разпоредби, като правилата на Комисията за ценни книжа и борси относно разкриването на информация за киберсигурността.

Ресурсите на вътрешния одит като средство за постигане на целите

Предизвикателствата в контекста на киберзаплахите, пред които се изправят организациите са големи, но вътрешният одит може да предостави уникална и независима гледна точка за рисковете на организацията и най-добрите начини за справяне с тях. Съветите, които упражняват активен мониторинг над проблемите на киберсигурността и се възползват изцяло от стойността, която може да предложи вътрешният одит, очаквано са в по-добра позиция за ефективно справяне с киберрисковете.

КАКВО ЛИПСВА В СЪВЕТА?

60% от организациите нямат ръководител „Киберсигурност“, който е член на Съвета или да е на ниво изпълнително управление.

59% от организациите посочват, че връзката между киберсигурността и бизнеса е в най-добрия случай неутрална, до характеризираща се с недоверие и несъществуваща.

20% от Съветите са убедени, че киберрисковете и предприетите в тяхната организация мерки за противодействие могат да защитят организацията от големи кибератаки.

36% от организациите твърдят, че киберсигурността се взима предвид още на етап планиране на нова бизнес инициатива.

Източник: *“The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency,”* IIA Global and EY, 30 Март, 2021.

[1] *Executive Perspectives on Top Risks for 2021 and 2030*, Protiviti and NC State University's ERM Initiative, 2021.

[2] *"Cybercrime to Cost the World $10.5 Trillion Annually by 2025"*, Steve Morgan, *Cybercrime Magazine*, November 13, 2020.

[3] *Cost of a Data Breach Report*, IBM, 2021.

[4] *"Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025"*, Gartner press release, January 28, 2021.

[5] *"Boards and Cybersecurity"*, McKinsey and Company podcast, February 2, 2021.

[6] *"Cybersecurity and the Role of Internal Audit: An Urgent Call to Action"*, Sandy Pundmann, Deloitte, 2017.

[7] *"Cybersecurity: An Evolving Governance Challenge"*, Harvard Law School Forum on Corporate Governance, March 15, 2020.

[8] *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures"*, Release Nos. 33-10459; 34-82746, Securities and Exchange Commission, February 26, 2018.

АНКЕТА

Има ли в Съвета на Вашата организация член с опит в киберсигурността?

- ❑ Да
- ❑ Не
- ❑ Не съм запознат

Посетете www.theiia.org/Tone, за да отговорите на въпроса и да се запознаете с резултатите от анкетата.

РЕЗУЛТАТИ ОТ АНКЕТА

На кого най-вече разчита Съветът за предоставяне на увереност относно ефективността на управлението на риска и вътрешния контрол?

Източник: Tone at the Top June 2021 survey.