RISK DOCTOR PARTNERSHIP BRIEFING

مدیریت ریسک جرایم سایبری

© May 2014, Ben Rendle

Ben.rendle@btinternet.com

جرایم سایبری تهدیدی با رشد سریع برای اقتصاد جهانی است. ولی به خوبی تعریف نشده و اغلب با جنگ سایبری یا تروریسم سایبری اشتباه گرفته می شود. متخصصین ریسک باید جرایم سایبری و ارتباط آن را با مدیریت ریسک بفهمند، به گونه ای که ما بتوانیم همکاری ارزشمندی در مهار کردن این تهدید مهم برای کسب و کار و جامعه داشته باشیم.

برخی از متخصصین ریسک گمان می کنند که جرایم سایبری تنها مرتبط با افراد فنی است و باید توسط واحد IT مدیریت شود. ولی جرایم سایبری ریسک مهمی را متوجه سازمان ها می سازد چرا که بر توانایی آنها در دستیابی به اهداف استراتژیک و عملیاتی تاثیر دارد. متاسفانه بسیاری از کسب و کارها نمی دانند ریسک سایبری چیست، احتمال متاثر شدن آنها چقدر است، گستره تاثیر چقدر می تواند باشد و بهترین روش برای مدیریت آن چیست.

جرایم سایبری می تواند یک سازمان را از راه های گوناگونی تحت تاثیر قرار دهد که عبارتند از:

- دزدی و تقلب آنلاین
- دزدی هویت
- اخاذی
- دزدی اطلاعات مشتری
- دزدی مالکیت معنوی
- جاسوسی صنعتی

میزان قرار گرفتن در معرض جرایم سایبری به سطح فعالیت های آنلاین سازمان، شامل محدوده حضور آنلاین آنها، سطح نگهداری آنلاین اطلاعات، قدرت امنیت آنلاین و درجه آگاهی از ریسک در فرهنگ سازمانی مرتبط است.

جهت مدیریت ریسک جرایم سایبری نخست باید سطح فعالیت های آنلاین خود را تعیین نماییم، تعیین نماییم که چه نوع فعالیت ها و دارایی هایی ممکن است تحت تاثیر جرایم سایبری قرار بگیرند. سپس می توانیم شناسایی، ارزیابی و مدیریت ریسک های جرایم سایبری را آغاز نماییم. مراحل زیر مثمرثمر خواهد بود:

- **درک واضح و شناسایی اهداف سازمانی برای فعالیت های آنلاین.** محیط های آنلاین متفاوت و خاص همواندانمان را تشخیص می دهیم و میزان تمایل آنها به ریسک آنلاین را ارزیابی می کنیم.
- **پیگیری عوامل فنی و فرهنگی.** اینها شامل موانع فرهنگی، مشکلات ارتباطی و تاثیرات انحراف در ادراک ها از ریسک های جرایم سایبری می باشند.
- **تشخیص تهدیدهای جرایم سایبری داخلی و خارجی.** تهدیدهای داخلی می تواند از خطاهای کارکنان، از دست دادن تصادفی داده ها یا درز کردن مخرب اطلاعات تجاری حساس باشد. تهدیدهای خارجی می تواند از هکر ها، گروه های فشار، رقبا یا حتا دولت های خارجی دشمن باشد و همچنین از ویروس ها و ...

- **مسوول، پاسخگو و مشوق هایی برای مهار ریسک های جرایم سایبری ایجاد نمایید.** همه کارکنان ارشد باید جهت مدیریت ریسک های جرایم سایبری در محدوده مسوولیت خودشان پاسخگو باشند و ما باید همواندانی را نیز که این را مشکل خودشان نمی دانند درگیر کنیم.
- **مدیریت ریسک های جرایم سایبری در چارچوب یک سیستم مدیریت ریسک سازمانی (ERM).** ریسک های جرایم سازمانی می توانند بر محیط های گسترده تری مانند اعتبار، استمرار کسب و کار تاثیر بگذارند و به زیرشاخه ها و تامین کنندگان نیز برسند، بنابراین باید به شکلی جامع به عنوان بخشی از پاسخ کلی ما به ریسک مهار شوند.
- **ایجاد دیدی جهانی برای تاثیرات ریسک جرایم سایبری.** بسیاری از سازمان ها به اقتصادهای برون مرزی برای تجارت، صادرات و تولید ثروت وابسته اند و این آنها را در معرض جرایم سایبری برون مرزی قرار می دهد که نمی توانند فراموش شوند.

ما به عنوان متخصصین ریسک، باید جرایم سایبری را در ذهن و عملکردمان در نظر بگیریم، به گونه ای که بتوانیم توصیه های کاربردی هدفمند به سازمانمان برای کاهش خطرات و حمایت از کسب و کار ارائه نماییم.