IRON MOUNTAIN®

KAMU SEKTÖRÜ İYİ UYGULAMA REHBERİ

ANCAK EN ZAYIF HALKANIZ KADAR GÜÇLÜSÜNÜZ

İnsan davranışlarının kurum içi risk yönetimindeki yerini Iron Mountain'ın araştırmasıyla keşfedin.

GİRİŞ

Son yıllarda sektörlerde yaşanan dalgalanmalar, kuruluşları saldırılara karşı dayanıklılıklarını ve risk stratejilerini yeniden düşünmeye yöneltti.

Bunu en somut şekilde kamu sektöründe görüyoruz. Kamu sektörü, dijital erişilebilirlik ve departmanlar arası iletişime duyulan ihtiyacın artmasıyla oluşan baskının benzeri görülmemiş bir dönüşüme yol açtığı başlıca örnek olarak karşımıza çıkıyor. İşsizlik davalarından aşı kayıtlarına kadar balon gibi büyüyen veri hacimleri ve esnek çalışmaya geçişle birlikte hızla otomatikleşen iş akışları, kamu operasyonları ve hassas veriler için güvenlik açığı riskinin çoğaldığı anlamına geliyor.

BİLİYOR MUSUNUZ?

Anketimize[1] göre, veri yöneticilerinin **neredeyse yarısı (%46)** pandemi sonucunda veri ihlali riskinin arttığını bildiriyor.

Peki bu tür siber saldırılar karşısında işinizi nasıl korursunuz?

Genellikle gözden kaçan önemli bir nokta, içerideki tehditler oluyor. Çoğunlukla kasıtsız olsa da, insan davranışı ve hatası şirketlere pahalıya mal oluyor - hassas bilgilerin kaybı ise kaçınılmaz bir sonuç olarak karşımıza çıkıyor. İç ve dış talepleri karşılama konusunda hızlı bir dijitalleşme yaşarken, kamu kuruluşları çok daha riskli durumda. Pandemiyle birlikte bu riskler gözler önüne serildi. Birçok departman çok daha fazla kişisel veri bulundurmaya başladı. Kamu kuruluşları uzaktan çalışmaya hazırlıksız yakalandığı için halka hizmet çabalarında strese girerek hata riskiyle karşı karşıya kaldı.

Yakın tarihli bir IBM raporu, bir kamu sektörü veri ihlalinin ortalama maliyetinin geçtiğimiz yıl içinde **1,08 milyon dolardan 1,93 milyon dolara** (%79 artış) yükseldiğini ortaya koydu[2].

Bu nedenle Iron Mountain, şirketlerin insan hatalarıyla bağlantılı potansiyel risk yönetimi alanlarını belirleyen EMEA genelinde bir çalışma[1] hazırladı ve bazı şaşırtıcı sonuçlar elde etti.

Hibrit ekipler arasında riskin nasıl yönetileceğine ve saldırılara karşı dayanıklılığı artıracak bir iş stratejisinin nasıl oluşturulacağına ilişkin içgörüler ve pratik ipuçları için okumaya devam edin.

1. Eylül 2021'de One Poll tarafından 10 ülkede 11.000 çalışanın katıldığı anket.
2. IBM Bir Veri İhlalinin Maliyeti Raporu, 2021.

BU KILAVUZDAKİ BÖLÜMLER

En kolay çözümden başlayalım.

Evde ve ofiste nasıl çalıştığımıza dair bazı şaşırtıcı gerçekler...

Bunlardan kaç tanesi **sizin için** de geçerli?

DAHA FAZLASI İÇİN İKONLARA 'TIKLAYIN'

Neyse ki, bu nispeten basit sorunlar düzeltilebilir. Bunları bir kez daha düşünün:

- Sorunu vurgulamak için bu istatistikleri 'parmakla göstermeden' paylaşın.
- Davranış değişikliğinin önemini vurgulayın.
- Yardımcı olabilecek araçları, bu konudaki eğitim ve desteği hatırlatın.
- Hesaplanmış ve gereksiz risk arasındaki farkı pekiştirin.
- Risk yönetiminin maksimum düzeyde anlaşılmasını ve ölçülmesini sağlamak için şirket politikalarınızı gözden geçirin.

RİSKE DUYARLI BİR KÜLTÜR YARATIN

2

İnsan doğasını değiştiremesek de, sıfırdan risk bilincine sahip bir kültür oluşturarak, riski yönetme şeklimizi inovasyonla düzeltebiliriz.

Riske karşı bütünsel bir dayanıklılık stratejisi oluşturmak için bu beş adıma göz atın:

1 ŞİRKETİNİZİN DÜŞÜNCE YAPISINI DEĞİŞTİRİN

GERÇEK:

Her üç çalışandan biri (%32) geçmişte **"kritik" bir hata yaptığını** belirtiyor ve %16'sı **şirketlerini maddi zarara sokan** bir risk aldığını söylüyor.

ÇÖZÜM:

Her çalışanı bir risk elçisi olarak yetkilendirip **risk farkındalığını iş kültürünüzün temeline yerleştirerek başlayın**. Bunun temel bir çalışan sorumluluğu olduğuna dair bir düşünce yapısı geliştirin. Bu düşünce yapısını tüm çalışanlara aşılayın.

STRATEJİK PLANINIZI OLUŞTURDUKÇA MADDELERİ **İŞARETLEYİN!**

2 BİLGİ YÖNETİMİ POLİTİKALARINIZI YENİDEN ŞEKİLLENDİRİN

GERÇEK:

Tüm çalışanların %37'si, dolandırıcılığa ya da kimlik avına maruz kalanlar da dahil (%20), **işte risk alınması gerektiğini düşünüyor**.

ÇÖZÜM:

Kamu kuruluşları, pandemi sebebiyle hızla yeni çalışma düzenine geçti. Ancak bu düzen artık iş akışı otomasyonu, mobil bağlantı ve bilgiye dijital erişim çerçevesinde uzun vadeli düşünülmesi gereken bir iş planına evrildi. Ofis, hibrit ve/veya uzaktaki çalışanlar ve üçüncü parti iş ortakları için geçerli, çerçevesi iyi çizilmiş bilgi yönetimi ilkeleri benimseyin.

Yasal olarak uzun süre saklama yükümlülüğünüz olan bilgi ve belgeler için dijital ve fiziksel bir arşive ihtiyacınız var. Bunun yanı sıra, **fiziksel belgeleri ve BT ekipmanlarını güvenli şekilde imha etmek** için güçlü bir plana sahip olmak büyük önem taşıyor.

3 DESTEKLEYİCİ BİR KÜLTÜR BENİMSEYİN

GERÇEK:

İnsanların %42'si işte yaptıkları **bir hata yüzünden strese giriyor**.

ÇÖZÜM:

Hibrit çalışma ortamlarının verimliliği artırdığı kanıtlanmış bir gerçek, ancak bazen yaşanan stres bu verimliliğe engel oluşturabiliyor. **İş akışlarınızın risk yönetimini kapsadığından emin olun**. Mortgage ve kredi başvuruları gibi süreçlerinizi düzenlemeye yardımcı olmak için **yapay zeka ve makine öğrenimi ile güçlendirilmiş yeni teknolojileri** değerlendirin.

"Bütünsel dayanıklılık" nedir?

Dayanıklılık - veya şirketinizin saldırıları savuşturma yeteneği - asla sonradan düşünülmemelidir. İş politikalarınızın ve süreçlerinizin her adımında yer almalıdır.

RİSKE DUYARLI BİR KÜLTÜR YARATIN 2

Pandemi sonrası teknoloji entegrasyonu

Konuştuğumuz veri yöneticilerinin yarısından fazlası (%59) pandemi sırasında **yeni bir yazılım satın aldı** ve üçte ikisi (%62) Microsoft Teams gibi **paylaşım araçları kullanmaya başladı**. Sohbetler ve toplantı kayıtları gibi yapılandırılmamış veriler için saklama süreleri büyük önem taşıyor. Bunun yanı sıra günümüz teknoloji ortamına uyarlanmış merkezi yasal uyum ve politika yönetimi sistemlerinin geliştirilmesi ve bu araçların bilgi yaşam döngüsü yönetimi programlarına dahil edilmesi gerekiyor.

4 SÜREÇLERİNİZİ GELİŞTİRİN

GERÇEK:

Konu işle ilgili veriler olduğunda çalışanların %47'si ofiste, evde olduğundan çok daha fazla **güvenlik bilincine sahip**.

ÇÖZÜM:

Devam eden modernizasyonla birlikte, hassas ve gizli bilgiler de dahil olmak üzere her zamankinden daha büyük veri hacimleri oluşturuluyor. Bu, erişim hakları yönetiminden dijital bilgi paylaşımına, veri saklama ve yapılandırılmamış verilerin yönetimine kadar **bilgi yönetimini tümüyle yeniden düşünmenizi gerektiriyor.** İlk adım olarak, verinin şirket içi ve dışında nasıl hareket ettiğini anlamak için bir veri haritası oluşturun.

5 EĞİTİMİNİZİ UNUTULMAZ KILIN

GERÇEK:

Veri yöneticilerinin %60'ı **risk yönetimi eğitimlerine** yüksek katılım sağlandığını söylerken, çalışanların %29'u eğitimlere hiç katılmadığını belirtiyor.

ÇÖZÜM:

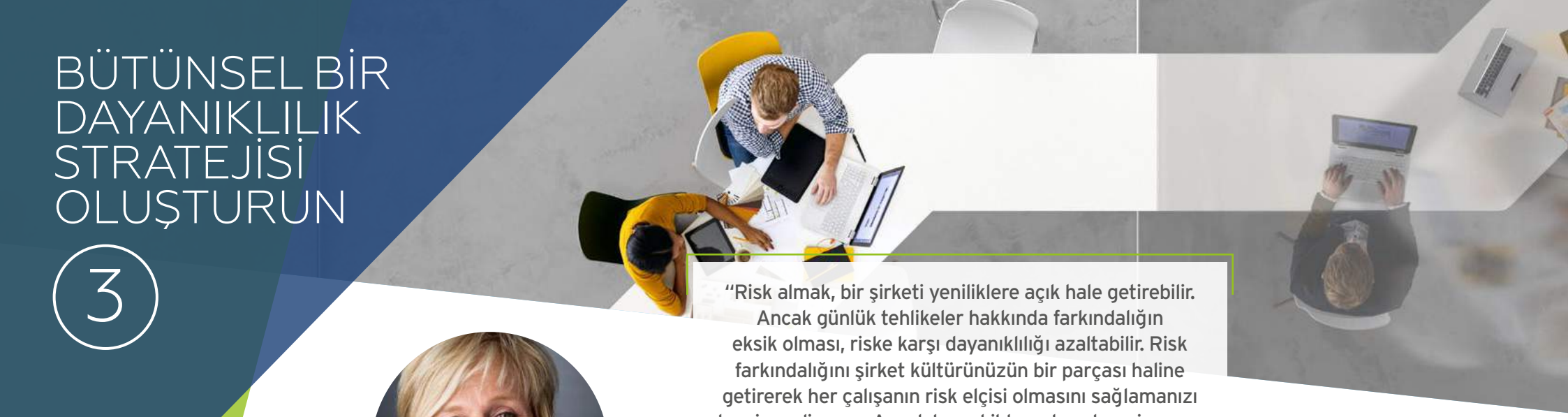
Şirketinizde risk yönetimi eğitimleriniz olsa da, araştırmalarımız bu eğitimlerin çabucak unutulduğunu gösteriyor. Etkiyi artırmak için **eğitimi daha ilgi çekici ve gerçek hayatla ilişkilendirilebilir** hale getirin. Böylece çalışanlar, risk yönetiminin kendilerini ve müşterilerini nasıl etkilediğini anlayabilir ve öğrendiklerini uygulamak için günlük risklerle karşılaşınca sorun yaşamazlar.

"Hepimiz insanız ve hata yaparız. Bu yüzden yaptığımız işlerde her zaman bir risk faktörü bulunur. Ama bu risk kalıcı değildir. Yeni iş modelleri, hibrit çalışma ve artan siber saldırı tehdidi, risklere karşı uzun vadeli dayanıklılığı sağlamak için şirket içi riskleri etkili bir şekilde yönetmeyi her zamankinden daha önemli hale getiriyor."

Sue Trombley, Düşünce Liderliği Yönetici Direktörü, Iron Mountain

BÜTÜNSEL BİR DAYANIKLILIK STRATEJİSİ OLUŞTURUN

3



"Risk almak, bir şirketi yeniliklere açık hale getirebilir. Ancak günlük tehlikeler hakkında farkındalığın eksik olması, riske karşı dayanıklılığı azaltabilir. Risk farkındalığını şirket kültürünüzün bir parçası haline getirerek her çalışanın risk elçisi olmasını sağlamanızı tavsiye ediyoruz. Ancak bu şekilde, çalışanların iş yapış şekillerinde yenilikler yapabilecekleri ve şirketlerin gelişebileceği güvenli bir alan yaratabilirsiniz."

Sue Trombley, Düşünce Liderliği Yönetici Direktörü, Iron Mountain

Anketimize göre, veri yöneticilerinin **%70'i** risk yönetiminden tüm çalışanların sorumlu olduğuna inanıyor.

Risklere karşı kalıcı bir dayanıklılık geliştirmek için risk stratejilerinizi iş süreçlerinizin her adımında uygulamalı, tüm çalışanların günlük eylemleriyle stratejinizi desteklemelerini sağlamalısınız. **Bunu "bütünsel dayanıklılık" olarak adlandırıyoruz.**

COVID-19'un etkilerinden kurtulmaya çalışan kamu kuruluşları, yapay zeka gibi yeni teknolojileri benimsemeye, dijital erişilebilirlik ve departmanlar arası iletişime yönelik sürekli artan taleplere yanıt vermeye çalışırken piyasadaki beklenmedik gelişmeleri ve riskleri de unutmamalıdır.

Hibrit çalışma çözümlerini risklere karşı dayanıklılık stratejileriyle bütünleştirmek, kamu kuruluşlarının uzun vadeli refahının anahtarıdır. Örneğin, herhangi bir yerden güvenli bilgi erişimine izin veren, işsizlik veya sosyal yardım taleplerinin işlenmesi için iş akışlarını kolaylaştıran ve verilerin tüm yaşam döngüsünün etkin bir şekilde yönetilmesine yardımcı olan, **bilgilerin gizli potansiyelini ortaya çıkaran** çözümler gibi...

Bilgi yönetimi konusundaki zorlukları aşmanıza ve hibrit çalışma düzeninde riske karşı dayanıklılığı artırmanıza yardımcı olacak çözümler için uzman ekibimizle iletişime geçebilirsiniz. Daha fazla bilgi için: ironmountain.com/tr

IRON MOUNTAIN HAKKINDA

1951 yılında kurulan Iron Mountain Incorporated (NYSE: IRM), saklama ve bilgi yönetimi hizmetlerinde dünya lideridir. Dünya çapında 225.000'den fazla kuruluş tarafından güvenilmektedir. 56 ülkedeki 1.450'den fazla tesiste 8,5 milyon metrekareyi aşan gayrimenkul ağıyla Iron Mountain, kritik bilgiler, son derece hassas veriler, kültürel ve tarihi eserler dahil olmak üzere maddi manevi çok değerli varlıkları saklıyor ve koruyor. Fiziksel arşiv yönetimi, bilgi yönetimi, dijital dönüşüm, güvenli imhanın yanı sıra veri merkezleri, bulut hizmetleri, sanat eseri saklama ve lojistiği içeren çözümler sunan Iron Mountain, işletmelerin maliyet ve risklerini düşürmelerine, düzenlemelere uymalarına, felaket durumlarından kurtulmalarına ve daha dijital bir çalışma ortamı benimsemelerine yardımcı oluyor. Daha fazla bilgi için www.ironmountain.com.tr adresini ziyaret edin.

+90 212 288 95 03 | IRONMOUNTAIN.COM/TR

IRON MOUNTAIN®