IRON MOUNTAIN®

SAĞLIK 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 sağlık sektöründe görüyoruz. Siber saldırılar, hastaların gizli verilerini riske atıyor. Bu arada, tıbbi kayıtların dijital platformlara taşınması, telesağlık ve nesnelerin interneti (IoT) cihazlarının giderek yaygınlaşmasıyla güvenlik açıkları da katlanarak artıyor.

BİLİYOR MUSUNUZ?

Mayıs 2021'de bir fidye yazılımı saldırısı **İrlanda'nın sağlık hizmetleri BT sistemlerini felç etti** ve ülkedeki hastanelerin çoğunu bir haftadan fazla bilgisayarsız bıraktı[1].

2020'de Avrupa'da bir hastaneye yapılan fidye yazılımı saldırısı, **hastalar için ciddi sonuçlar** doğurdu[2].

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 sağlık kuruluşlarını ve hastaları riske atıyor ve finansal kayıplara neden oluyor. Hassas tıbbi bilgilerin kaybedilmesi durumunda önemli itibar kayıpları da kaçınılmaz bir sonuç olarak karşımıza çıkıyor. Böylesine hızlı bir dijitalleşme döneminde, sağlık kuruluşları çok daha riskli durumda.

Yakın tarihli bir IBM raporu, bir sağlık hizmeti veri ihlalinin ortalama maliyetinin ihlal başına **9,23 milyon dolar** olduğunu tahmin ediyor. Bu tutar, diğer tüm sektörlerden daha fazla[3].

Bu nedenle Iron Mountain, şirketlerin insan hatalarıyla bağlantılı potansiyel risk yönetimi alanlarını belirleyen EMEA genelinde bir çalışma[4] 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. Fidye yazılımı saldırısından 10 gün sonra, İrlanda sağlık sistemi mücadele etmeye devam ediyor.
2. Yeni Zelanda Hastanesi, büyük siber saldırının ikinci haftasında hala iş kesintisiyle karşı karşıya.
3. IBM Bir Veri İhlalinin Maliyeti Raporu, 2021.
4. Eylül 2021'de One Poll tarafından 10 ülkede 11.000 çalışanın katıldığı anket.

BU KILAVUZDAKİ BÖLÜMLER

1 HIZLI ÇÖZÜM

2 RİSKE DUYARLI BİR KÜLTÜR YARATIN

3 BÜTÜNSEL BİR DAYANIKLILIK STRATEJİSİ OLUŞTURUN

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:

Sağlık kuruluşları, pandemiye karşı acil müdahalele planları oluşturdu, ancak bu düzen artık hibrit çalışma çerçevesinde uzun vadeli düşünülmesi gereken bir iş planına evrildi. Ofiste çalışanlar, hibrit çalışanlar, uzaktan çalışanlar ve üçüncü parti iş ortakları için **kapsamı belirlenmiş, iyi bir bilgi yönetimi planı** oluşturun.

Sağlık kuruluşları, hasta kayıtlarını dijitalleştirmeye hızla devam ederken, tüm arşivleme, taşıma, dijitalleştirme ve elden çıkarma süreçleri boyunca güçlü bir gözetim zinciri sağlamak 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**. Süreçlerinizi düzenlemeye yardımcı olmak için yapay zeka ve makine öğrenimi ile güçlendirilmiş yeni teknolojileri değerlendirin. Böylece personeliniz gelişmiş hasta bakımı hizmeti sunmaya odaklanabilir.

"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**. Hastalarla 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:

Dijital kayıtlar ve online danışmanlık hizmetlerinin hızla norm haline gelmesiyle birlikte, her zamankinden daha büyük hacimlerde veri 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:

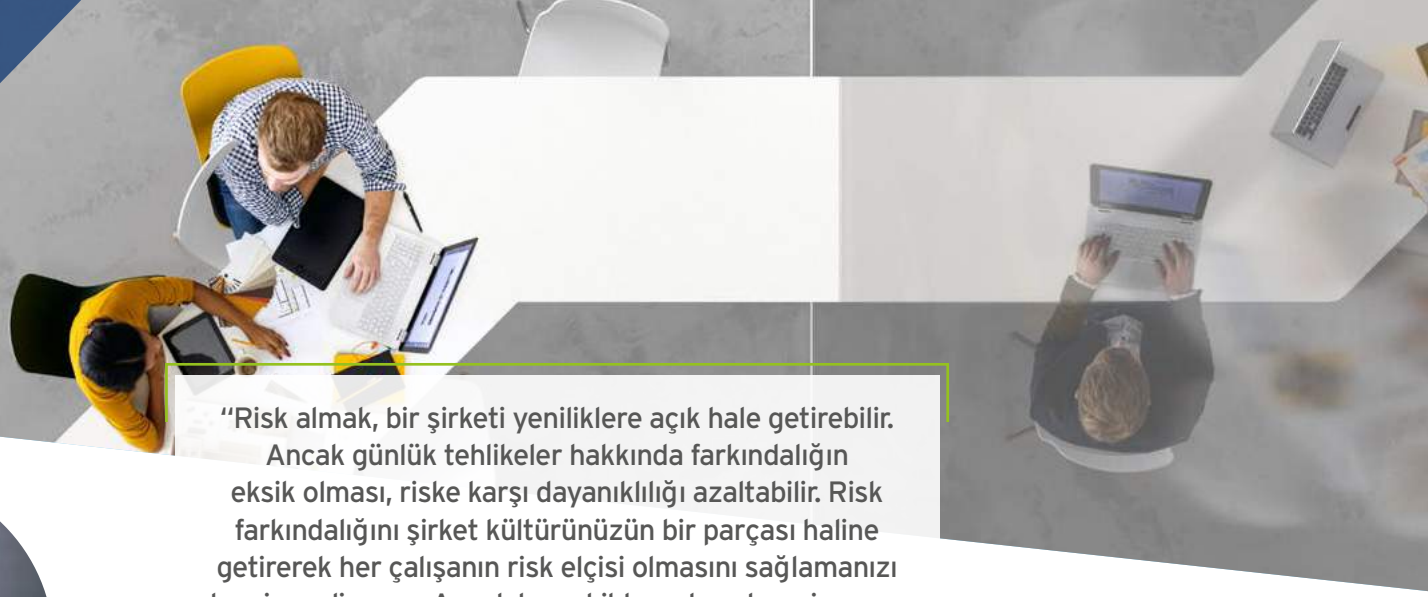
Risk yönetimi eğitimleriniz olsa da, araştırmalarımız bu eğitimlerin çabucak unutulduğunu gösteriyor. Etkiyi artırmak için **eğitimi daha ilgi çekici ve gerçek hayatla ilişkilendirilebilir** hale getirin. Böylece çalışanlar, risk yönetiminin kendilerini ve hastaları nasıl etkilediğini anlayabilir ve 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 kliniklerdeki ve idari alandaki iş süreçlerinizin her adımında uygulamalı, tüm çalışanların günlük eylemleriyle stratejinizi desteklemelerini sağlamalısınız. **Bunu "bütünsel dayanıklılık" olarak adlandırıyoruz.**

Sağlık kuruluşları operasyonlarını hızlıca dijitalleştirip COVID-19'un etkilerinden kurtulmaya çalışırken piyasadaki beklenmedik gelişmeleri ve riskleri de unutmamalıdır.

Hibrit çalışma çözümlerini risklere karşı dayanıklılık stratejileriyle bütünleştirmek, sağlık kuruluşlarının uzun vadeli refahının anahtarıdır. Örneğin, herhangi bir yerden güvenli bilgi erişimine izin veren, hasta işlemleri için iş akışlarını kolaylaştıran, biçimi veya türü ne olursa olsun verilerinizin tüm yaşam döngüsünü etkin bir şekilde yönetmeye yardımcı olan, **bilgilerinizdeki gizli anlamı ortaya çıkarmanızı** ve bu bilgileri kuruluşunuz için daha verimli kullanmanızı sağlayan 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/industries/healthcare-services.

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®