Por Nicole Mendolera (*)

Os sistemas de saúde em todo o mundo estão em uma corrida contra o tempo para garantir equipamentos médicos, localizar camas extras para cuidados intensivos e expandir sua força de trabalho clínica, recrutando inclusive profissionais de saúde aposentados. Os médicos estão isolando e tratando pacientes da COVID-19, encontrando soluções criativas para a escassez de dispositivos médicos e cuidando de outros pacientes gravemente doentes – tudo isso, enquanto tentam evitar um aumento nos incidentes de cibersegurança.

Com a segurança e o cuidado do paciente sendo prioridades máximas, os sistemas de saúde querem garantir que questões críticas não sejam negligenciadas, uma vez que respondem ao surto nos casos da COVID-19. Para oferecer os melhores resultados aos pacientes, os médicos devem ter acesso a dados seguros e precisos no momento em que elaboram planos de tratamento. Com mais dispositivos médicos conectados, como bombas intravenosas automatizadas, que transmitem dados dos pacientes em tempo real para os médicos, a cibersegurança dessas tecnologias é mais crítica agora do que nunca.

A segurança permite o monitoramento e o cuidado com o paciente, preservando a exatidão dos dados, ao mesmo tempo em que protege a confidencialidade e a privacidade do mesmo. Um ciberataque que torne os dados dos pacientes inacessíveis aos médicos, ou desabilite os dispositivos, pode ser tão prejudicial para os esforços de combate à COVID-19, quanto a escassez de profissionais.

Por meio do trabalho em equipe com organizações de saúde, que estão lutando contra a COVID-19, identificamos oito questões que são regularmente negligenciadas à medida que essas empresas respondem às pressões da pandemia. A seguir, dividimos alguns conselhos em relação às principais iniciativas que os líderes de saúde podem tomar para proteger áreas que podem ter sido negligenciadas:

1) Se proteja e responda ao aumento dos ataques cibernéticos

A COVID-19 fez dos sistemas de saúde um alvo de ataques cibernéticos.

Se familiarize com a nova onda de ataques cibernéticos que tem como alvo o seu sistema de saúde. Esses ataques incluem, mas não estão limitados a esquemas de fraude, ataques de negação de serviço, tentativas de roubar informações de pacientes com o objetivo de cometer fraude de seguros, e o uso de contas nas redes sociais para distribuir material malicioso.

Restabeleça a linha de tráfego de rede necessária para detectar ataques. As linhas de base de tráfego de rede vão mudar significativamente à medida que a sua força de trabalho adota o trabalho remoto, e novos profissionais de saúde se preparam para ajudar durante a crise. Recalibre as configurações de monitoramento de segurança de acordo com suas necessidades.

Prepare-se para reagir rapidamente a um incidente cibernético, validando os procedimentos de resposta e escalonamento ao lidar com ataques de segurança.

2) Gerenciar o aumento significativo do trabalho remoto

Os colaboradores não essenciais estão trabalhando de casa, ao invés de ir até seus escritórios, enquanto um grande número de médicos aposentados e estudantes de medicina têm se organizado para ajudar.

Imponha o uso de soluções de trabalho remoto seguro, incluindo redes privadas virtuais (VPN) e autenticação multifator.

Emita diretrizes de trabalho remoto e incentive o uso de plataformas colaborativas, como ferramentas de videoconferência, portais seguros e unidades compartilhadas protegidas.

Forneça links para recursos oficiais sobre a pandemia tais como agências governamentais e aumente o envio de mensagens organizacionais para manter os trabalhadores bem informados.

Entenda os riscos e implemente controles compensatórios (por exemplo, maior monitoramento) e quando for preciso adiar atualizações de software críticas, coloque os dispositivos médicos em redes não segmentadas.

Forneça uma atualização para o staff responsável pelo atendimento e suporte sobre engenharia social e protocolos de privacidade, pois eles verão um aumento no número de ligações dos pacientes.

3) Se defendendo contra ataques de phishing

Tem havido um aumento de e-mails de phishing e spam que usam a COVID-19 como tópico. Estes e-mails são particularmente dirigidos a executivos corporativos e usam a pandemia para enfatizar a urgência do seu pedido.

Destaque a questão dos ataques de phishing aos seus executivos, e à sua organização de forma mais ampla. Certifique-se de que os funcionários saibam quem devem contatar se tiverem dúvidas ou suspeitas.

Educar os usuários finais sobre como eles podem distinguir os e-mails reais de e-mails de phishing. Forneça materiais contínuos de conscientização de segurança e lembretes para a sua força de trabalho durante a pandemia.

Assegure que o rastreamento e o inventário dos dispositivos permaneçam atualizados para que eles possam ser alocados onde são mais necessários.

Priorize as vulnerabilidades que requerem uma correção imediata. Altere a senha padrão dos dispositivos médicos e evite conectar dispositivos com vulnerabilidades de alto risco conhecidas à rede. Use patches de software para corrigir vulnerabilidades de execução de código remoto dentro de redes privadas.

4) Minimize o tempo de inatividade dos dispositivos médicos

Os dispositivos médicos que estiveram em depósitos podem não estar prontos para uso imediato. Avalie os dispositivos médicos que não estão em uso atualmente para determinar sua operabilidade – eles podem não ter recebido as atualizações mais recentes ou não ter sido checados sobre a necessidade de eventuais recalls.

Assegure que o rastreamento e o inventário dos dispositivos permaneçam atualizados para que eles possam ser alocados onde são mais necessários. Priorize as vulnerabilidades que requerem uma correção imediata. Altere a senha padrão dos dispositivos médicos e evite conectar dispositivos com vulnerabilidades de alto risco conhecidas à rede. Use patches de software para corrigir vulnerabilidades de execução de código remoto dentro de redes privadas.

5) Estabilize a sua rede

A infraestrutura que suporta os sistemas de saúde não foi projetada para acomodar o aumento do tráfego na rede como o que está ocorrendo durante a pandemia da COVID-19.

Verifique se a sua infraestrutura atual tem capacidade para suportar o aumento do tráfego e um maior número de utilizadores remotos. Implemente dispositivos de rede adicionais, garanta largura de banda extra, e compre licenças e ferramentas, conforme for necessário.

Acelere o onboarding do staff médico que já aposentou, mas que está voltando ao trabalho. Garanta apenas o acesso adequado e necessário aos sistemas, conforme exigido para fazer o trabalho de cada um deles.

Considere a criação de centros de ajuda adicionais para apoiar o provável fluxo de perguntas dos pacientes.

6) Impulsione os seus fornecedores

Os fornecedores de equipamento médico essencial estão sob pressão para entregar, quando as suas próprias cadeias de suprimento estão sendo demandadas, e seus colaboradores correm o risco de adoecer ou de ficar em autoisolamento.

Checar proativamente seus fornecedores para compreender se a escassez de equipamento médico crítico vai afetar seu negócio de alguma maneira.

Confirmar os prazos de entrega do fornecedor e procurar fornecedores alternativos que possam ser capazes de ajudar se os problemas de escassez forem previstos. Para esse último, tenha cuidado– a Interpol alertou sobre criminosos que aplicam fraudes financeiras, se fazendo passar por distribuidores médicos, afirmando vender máscaras e outros suprimentos.

Seja persistente em defender, junto ao governo, os suprimentos necessários para proteger seus colaboradores e tratar os seus pacientes.

Procure em sua comunidade por suprimentos adicionais. Aproxime-se das organizações e profissionais locais, como dentistas e empresas de construção civil, bem como do público, que podem ter suprimentos para doar.

7) Saiba lidar com tomadas de decisões críticas quando os líderes não estão presentes

Os principais líderes empresariais e médicos podem adoecer e ficar indisponíveis para tomar decisões críticas.

Confirme as funções essenciais para apoiar a segurança dos pacientes durante uma crise e o pessoal que gerencia e executa os processos críticos.

Identifique backups/delegue funções para os tomadores de decisão que adoecerem e assegure que eles tenham acesso à documentação, ferramentas e formação que lhes permitam tomar decisões de maneira bem informada.

Comunique frequentemente sobre qualquer mudança de pessoal. Isto inclui líderes empresariais, médicos e aqueles em funções-chave de apoio, tais como folha de pagamento, compras e TI.

8) Ofereça segurança e apoio por meio de comunicações direcionadas

Durante uma pandemia, a ansiedade e o pânico estão no auge. Seu pessoal e seus pacientes querem saber se você está fazendo todos os esforços necessários para apoiá-los fisicamente, mentalmente e financeiramente.

Minimize a desinformação oferecendo à sua força de trabalho e aos pacientes recursos confiáveis que eles podem usar para se manterem atualizados sobre a COVID-19 e seu potencial impacto sobre eles e suas famílias.

Aumente o apoio aos funcionários, por exemplo, ajustando as políticas de licenças por doença pagas, gerenciando uma linha direta para crises de saúde mental ou oferecendo assistência financeira.

Forneça atualizações regulares sobre como você está apoiando sua força de trabalho e seus pacientes em tópicos-chave (por exemplo, como você está mantendo seus médicos seguros ao lidar com a falta de equipamentos).

(*) **Nicole Mendolera** é Gerente de Cybersecurity e Resiliência Empresarial da EY America.

Artigo publicado no Guia de Plataformas e Soluções para o Combate à Covid-19, edição especial da Medicina S/A. **Faça o download gratuito da edição clicando aqui**.

Fonte: Medicina S/A, em 03.07.2020