إدارة السمعة الرقمية والاستجابة للأزمات السيبرانية

الإمارات العربية المتحدة - دبي

2026 / 08 /20 – 16

مقدمة:

في عصر السيادة الرقمية وتطبيق مبدأ تصفير البيروقراطية، لم تعد الأزمة السيبرانية مجرد تحدٍ تقني، بل هي اختبار مباشر لسمعة المؤسسة وموثوقية الدولة في الفضاء الرقمي. تهدف هذه الدورة إلى تمكين القادة من بناء "درع حصانة رقمي" يدمج بين الاستجابة التقنية السريعة والاتصال الاستراتيجي الذكي. يركز البرنامج على كيفية إدارة السمعة أثناء الاختراقات الأمنية أو تسريب البيانات، مع ضمان النزاهة المطلقة والشفافية، مما يضمن ريادة المؤسسة وقدرتها على تحويل الأزمة السيبرانية إلى فرصة لتعزيز الثقة الرقمية والريادة العالمية.

أهداف الدورة:

- استيعاب مفاهيم **السمعة السيبرانية السيادية** وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية الأمنية.
- تطوير مهارات هندسة "الاتصال الدفاعي" لحماية السمعة أثناء وبعد الحوادث السيبرانية.
- إتقان فن إدارة المعلومات المتسربة (Data Leaks) إعلامياً لضمان النزاهة وحماية الخصوصية.
- حوكمة مخرجات "فرق الطوارئ المشتركة" (التقنية والإعلامية) لضمان وحدة الرواية الرسمية.
- اكتساب مهارات **تصفير زمن الاستجابة** عبر أتمتة مسارات التواصل والتحقق الرقمي.
- تعزيز السيادة الرقمية من خلال حماية الهوية الرقمية للجهة من الانتحال أو التزييف العميق.
- تطبيق استراتيجيات "الصدق الرقمي" لاستعادة الثقة بعد الهجمات الإلكترونية بنزاهة تامة.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بـ "الإفصاح المسؤول" عن الثغرات الأمنية.
- صياغة خارطة طريق شاملة لبناء منظومة "صمود رقمي" تحمي السمعة وتدعم جودة الحياة.

محتويات الورشة:

اليوم الأول:

فلسفة السمعة في عصر الأزمات السيبرانية

الرشاقة القيادية وهندسة الثقة الرقمية

- مفهوم السمعة السيبرانية: لماذا يُعد "الانطباع الرقمي" أهم من "الخوادم التقنية"؟
- مواءمة إدارة الأزمات مع استراتيجية تصفير البيروقراطية: كيف نلغي عوائق تدفق المعلومات بين الأقسام التقنية والإعلامية؟
- تحليل العلاقة بين "الشفافية الأمنية" وبين بناء المصداقية الوطنية عالمياً.
- تمرين "رادار التهديدات": تحديد الثغرات الاتصالية التي قد تتسبب في انهيار السمعة أثناء الاختراق.

النزاهة والسيادة في بناء السردية الدفاعية

- مفهوم "السيادة المعلوماتية": حماية الرواية الرسمية من التلاعب أو "البروباغندا" السيبرانية المعادية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة والصدق في الإفصاح عن حجم الاختراق.
- سيكولوجية الثقة بعد الهجوم: بناء المصداقية عبر "النزاهة الرقمية" والعدالة في إبلاغ المتضررين.
- صياغة ميثاق "الاتصال السيبراني المسؤول" لضمان توافق الردود مع الهوية والسيادة الوطنية.

اليوم الثاني:

السيادة التقنية وإدارة المعلومات في الوقت الفعلي

الأمان الرقمي والخصوصية كركيزة لإدارة السمعة

- أخلاقيات التعامل مع "البيانات المسربة": حدود الكشف والسرية في الأنظمة السيادية.
- الأمان الرقمي كمتطلب للسمعة: حماية "قنوات النشر" من الانتحال أثناء الأزمة السيبرانية.
- إدارة الهوية الرقمية (UAE Pass) وأثرها على موثوقية البيانات الرسمية وتصفير مخاطر "التزييف".
- تمرين تقني: تصميم بروتوكول "التحقق المزدوج" لضمان نزاهة البيانات قبل نشرها للجمهور.

أخلاقيات التفاعل مع أنظمة الذكاء الاصطناعي في الأزمات

- حدود استخدام الذكاء الاصطناعي في رصد "هجمات السمعة" دون انتهاك السرية أو القيم.
- حوكمة مخرجات أنظمة "التحليل التنبؤي للأزمات": الضمان الأخلاقي لعدم التضليل.
- مفهوم "الأمانة في الرصد": تجنب إخفاء الحقائق التقنية خلف مبررات خوارزمية غير دقيقة.
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في "تأمين السمعة" من الهجمات الممنهجة.

اليوم الثالث:

الحياد والعدالة في الاستجابة للأزمات السيبرانية

النزاهة الرقمية ومكافحة "حروب المعلومات" والتضليل

- أخلاقيات "الحقيقة الرقمية": دور القائد في حسم الجدل حول الاختراقات ببيانات نزيهة.
- الرقابة الأخلاقية على أنظمة "الرد السريع": كيف نضمن الشفافية والعدالة في معالجة مخاوف المتعاملين؟
- تطبيق قاعدة "الإرادة البشرية القيادية": التدخل لتصحيح مسار "بلاغ آلي" قد يسبب قلقاً غير مبرر.
- حساب معامل الثقة في الأنظمة التقنية لتقليل احتمالات الخطأ الناتج عن "الهلوسة الرقمية."

حوكمة المسؤولية عن مخرجات إدارة الأزمات الذكية

- المسؤولية المهنية للقائد عند حدوث "انحراف في السمعة" ناتج عن أتمتة الردود الأمنية.
- إدارة العلاقة مع المنصات العالمية: ضمان السيادة والشفافية في معالجة المحتوى الذي يمس الأمن الوطني.
- بناء أنظمة "التحقق المزدوج" لضمان عدم غياب الحكمة البشرية في القرارات الاتصالية المصيرية.
- تمرين محاكاة: إدارة أزمة سمعة ناتجة عن "تسريب بيانات" تم تضخيمه عبر حسابات وهمية.

اليوم الرابع:

المسؤولية المهنية وإدارة "التعافي الرقمي"

القيادة الاتصالية وإدارة السمعة في بيئة هجينة

- أخلاقيات إدارة أزمات السمعة السيبرانية: الموازنة بين "سرعة الرد" وبين الوقار والسيادة الحكومية.
- الرقابة على "البصمة الرقمية للجهة" وأثرها على حيادية ومصداقية القرار السيادي والقانوني.
- بناء نظام "الإفصاح الاستباقي": ضمان الشفافية المطلقة لتصفير فرص انتشار "الأجندات الخارجية."
- التدقيق الأخلاقي على سلاسل "إنتاج الخطاب الأمني" لضمان خلوها من الممارسات غير العادلة.

أخلاقيات الاستجابة لـ "التزييف العميق" والاختراقات الدولية

- المسؤولية الأخلاقية في التبليغ عن الثغرات التقنية التي قد تسبب "أزمة سمعة" وطنية.
- فن التواصل الأخلاقي أثناء تعطل القنوات الرسمية: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل.
- إدارة "التعافي الذهني للجمهور": إجراءات إعادة بناء الصورة بعد رصد انحراف في الانطباع العام.
- بناء خطة "الحصانة السيبرانية الشاملة": تحصين منظومة السمعة ضد الهجمات الإعلامية الممنهجة.

اليوم الخامس:

مختبر الابتكار المهني وصناعة نموذج "الصمود الرقمي" الريادي

التطبيق العملي وتصفير البيروقراطية في أنظمة الاستجابة والتعافي السيبراني والتميز

- تطوير خارطة الطريق التنفيذية لدمج أدوات الاتصال الدفاعي الذكي في الممارسات اليومية بمرونة ورشاقة تضمن استمرارية الثقة والتميز والنمو.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ النزاهة السيبرانية لضمان استدامة الشفافية والوضوح في التعامل مع حوادث تسريب البيانات والريادة العالمية.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية (مثل فئات الأمن السيبراني والحوكمة الرقمية) مع التركيز على الابتكار في إدارة "درع الحصانة" والنمو.
- تمرين مختبر المحاكاة لإدارة المعضلات التقنية والاتصالية المعقدة (مثل اختراق الهوية الرقمية للجهة) وصياغة الحلول الاستباقية الناجحة والتميز الشامل.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية "حصانة سيبرانية" تضمن نزاهة السمعة الحكومية بنسبة 100.%
- القدرة على هندسة منظومات استجابة استباقية بمرونة وتوافق مع متطلبات السيادة الوطنية.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي.
- بناء سجل ممارسات فضلى في إدارة المعلومات تحت الضغط السيبراني يدعم اتخاذ القرار القيادي الآمن.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في الحوكمة والاتصال.

الفئة المستهدفة:

- القيادات العليا ومدراء إدارات الاتصال الحكومي، الأمن السيبراني، وتقنية المعلومات.
- مسؤولو الحوكمة، المخاطر، والتميز المؤسسي في الجهات السيادية والاتحادية.
- مستشارو الإعلام الاستراتيجي، الخبراء القانونيون، ومدراء السمعة المؤسسية.
- رؤساء فرق مشاريع تصفير البيروقراطية وتطوير منظومات الاستجابة السريعة للأزمات.
- الكوادر الطموحة الساعية لامتلاك جدارات "قائد إدارة السمعة السيبرانية النزيه."

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)